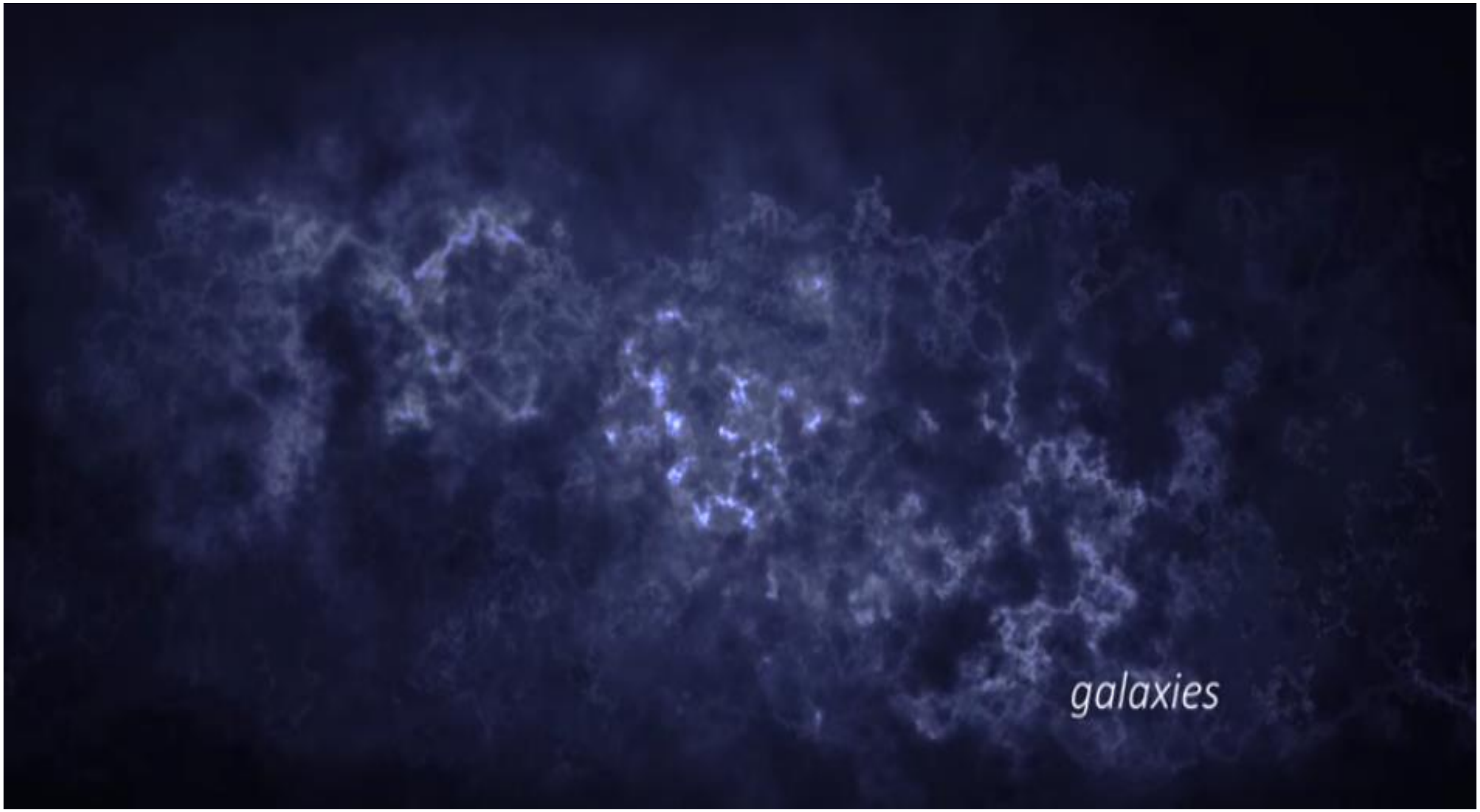
COMPUTER NETWORKS
18CS46

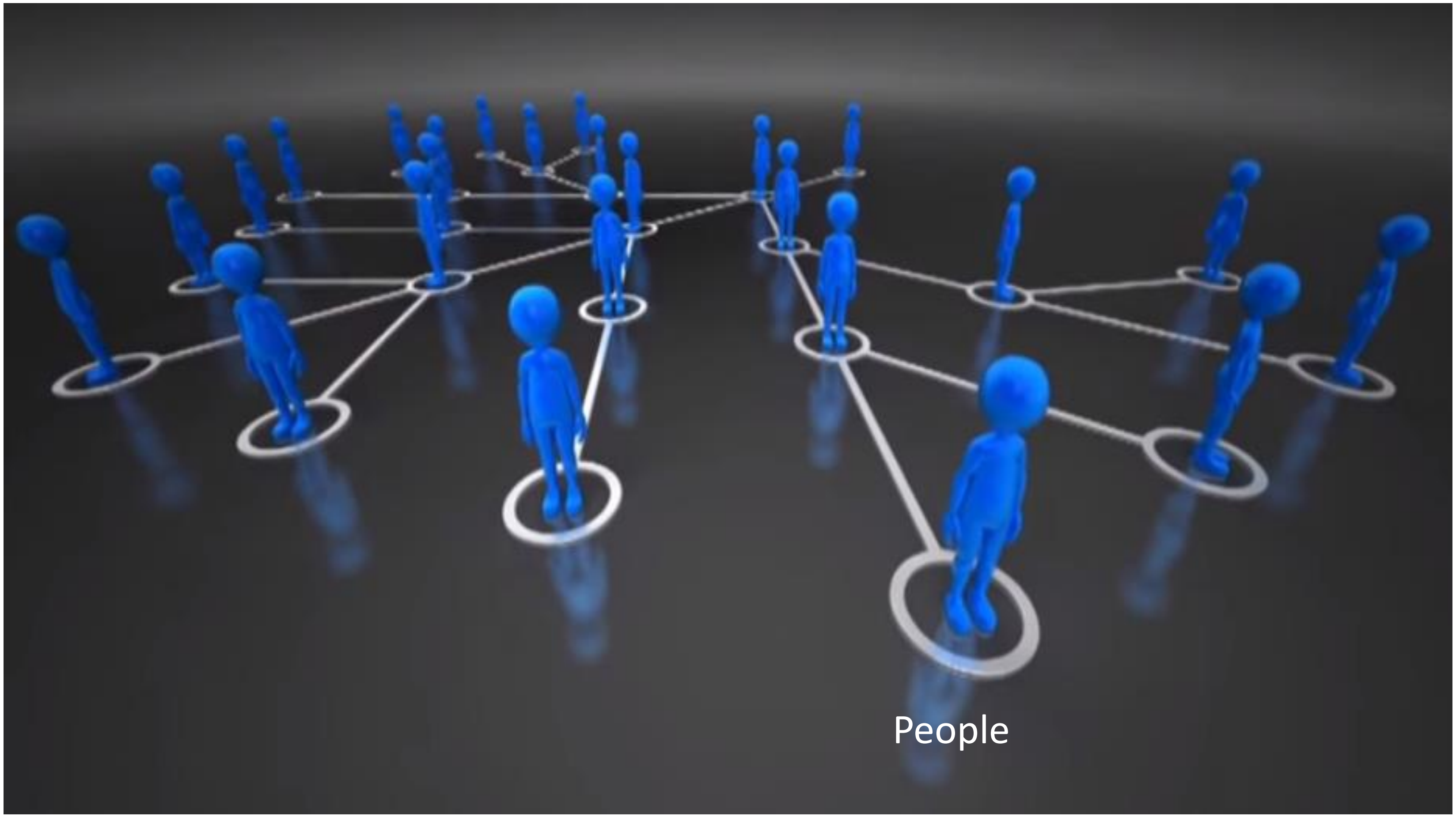
Dr. Minal Moharir

Connectivity

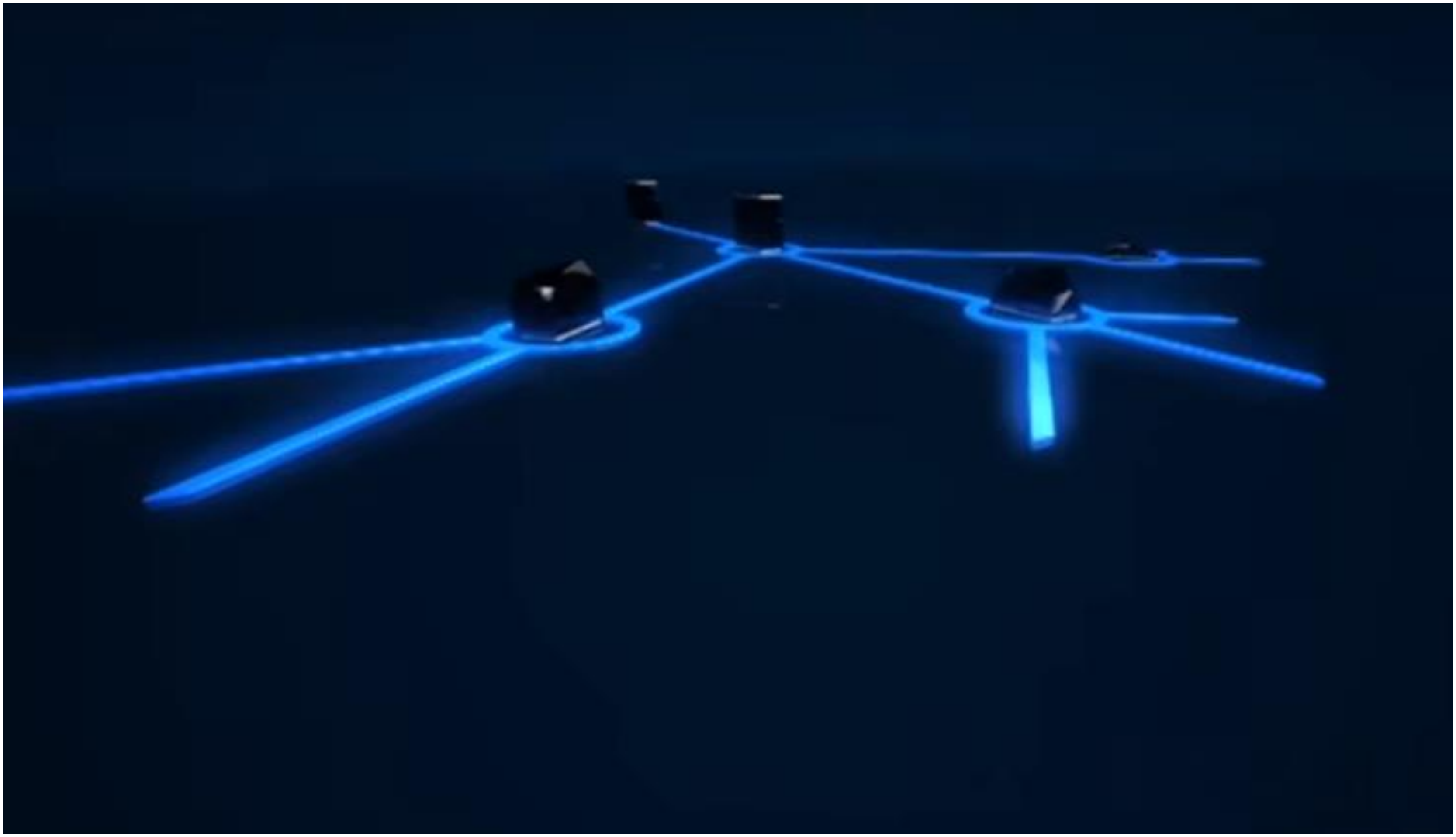


Connectivity

Connectivity



Connectivity



Network Models & Layered Architecture

a network :

sends data from one location to another

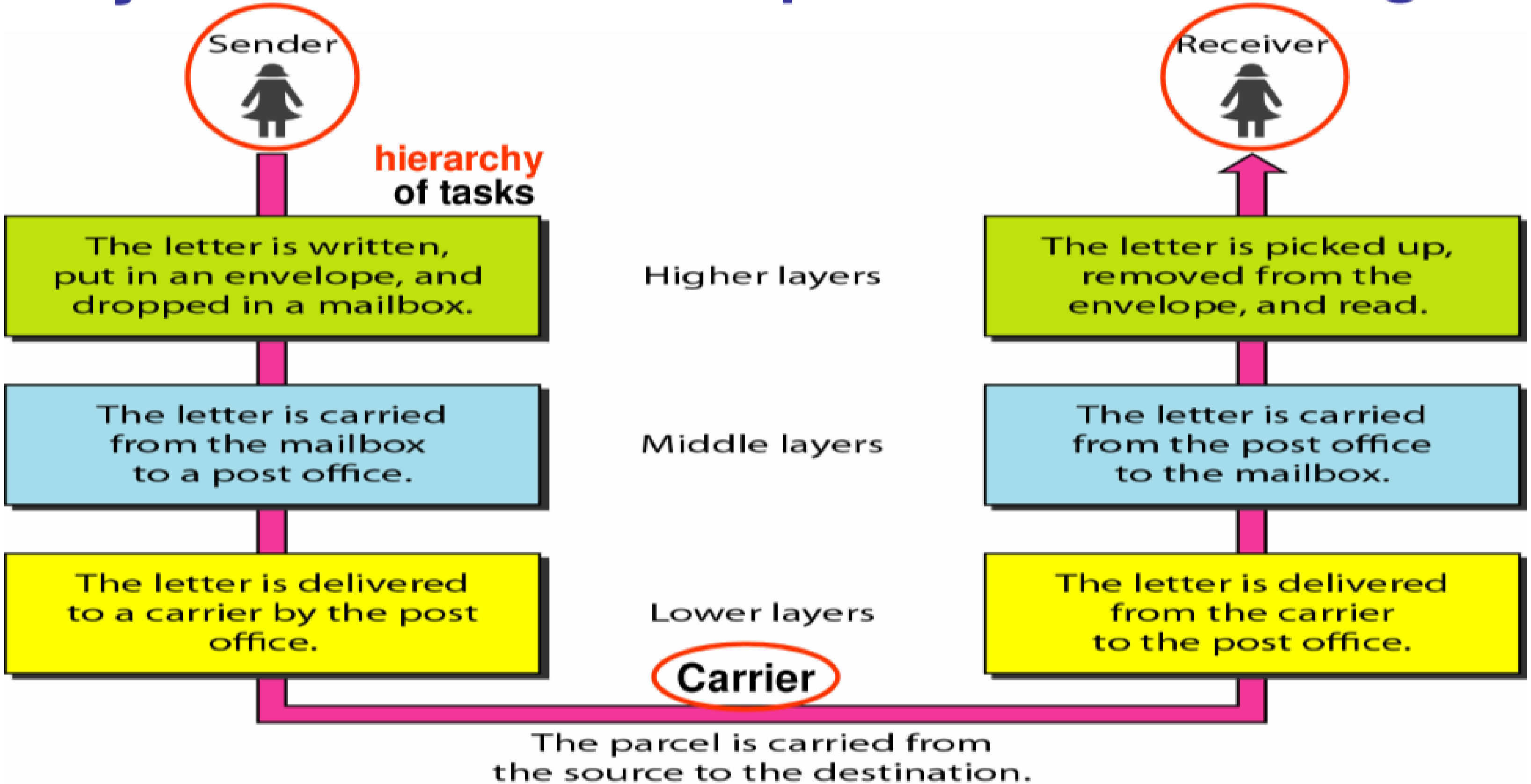
consists of hardware and software

hardware : physical equipment that carries signal from one point of network to another

software : consists of instruction sets that provide the expected services

Network Models & Layered Architecture

Layered Tasks : example of letter exchange



lower layer provides services to the layer immediately above it

Network Models & Layered Architecture

Layered Tasks : example of letter exchange

hierarchy of tasks

tasks must be done in the order given in the hierarchy

each layer uses the services of the layer below it

Network Models & Layered Architecture

Network Architecture

network design / architecture must be able to accommodate changes in :

- underlying technologies upon which they are based

- demands placed by the application programs

Network Models & Layered Architecture

Network Architecture

monolithic organisation is inflexible, obsolescence-prone

layered methodology for flexibility and growth with changing requirements

each layer carries out a specific set of communication using its own protocol and builds on the services of layer below it

Network Models & Layered Architecture

Network Architecture

end-to-end communication needs to be segmented into layers

interaction between layers is to be clearly defined

each layer is functionally independent and can be modified based on changing needs

Network Models & Layered Architecture

Network Architecture

common functions are grouped into related & manageable sets - *layers*

functional layers for :

- **data transportation**
- **routing of packets across multiple hops**
- **transfer of data frame from one physical interface to another**

Network Models & Layered Architecture

Computer Networks : Layered Models

in the context of computer networks two layered models are relevant :

OSI model

TCP/IP model

Network Models & Layered Architecture

OSI model

the open systems interconnection (OSI) model of the international standards organization (ISO)

an open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture

OSI model is designed for understanding and designing a network architecture that is flexible, robust and interoperable

Network Models & Layered Architecture

OSI model

contains seven separate, ordered layers

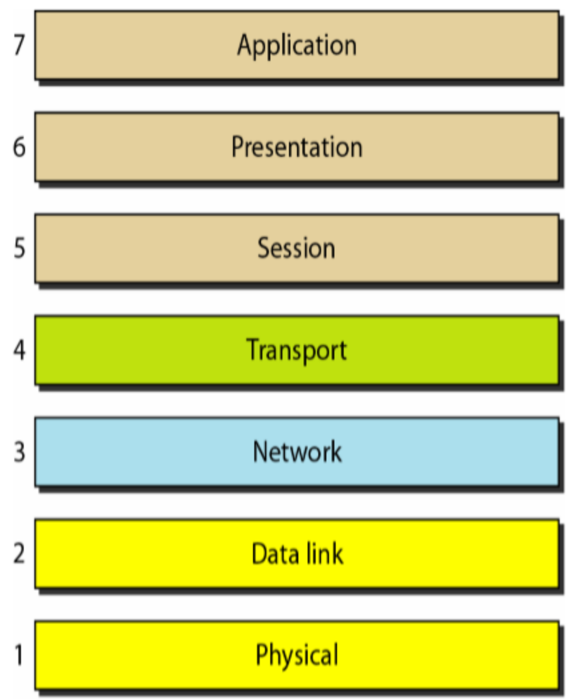
networking functions that have related uses are collected into discrete groups to form layers

each layer defines a part of the process of moving information across a network

each layer defines a function distinct from those of the other layers

Network Models & Layered Architecture

OSI model



each layer is expected to provide services to the layer above it

specific implementation of functions of a layer can be modified or replaced without requiring changes to the other layers

Network Models & Layered Architecture

OSI model

architecture is comprehensive and flexible

allows complete interoperability between heterogeneous systems

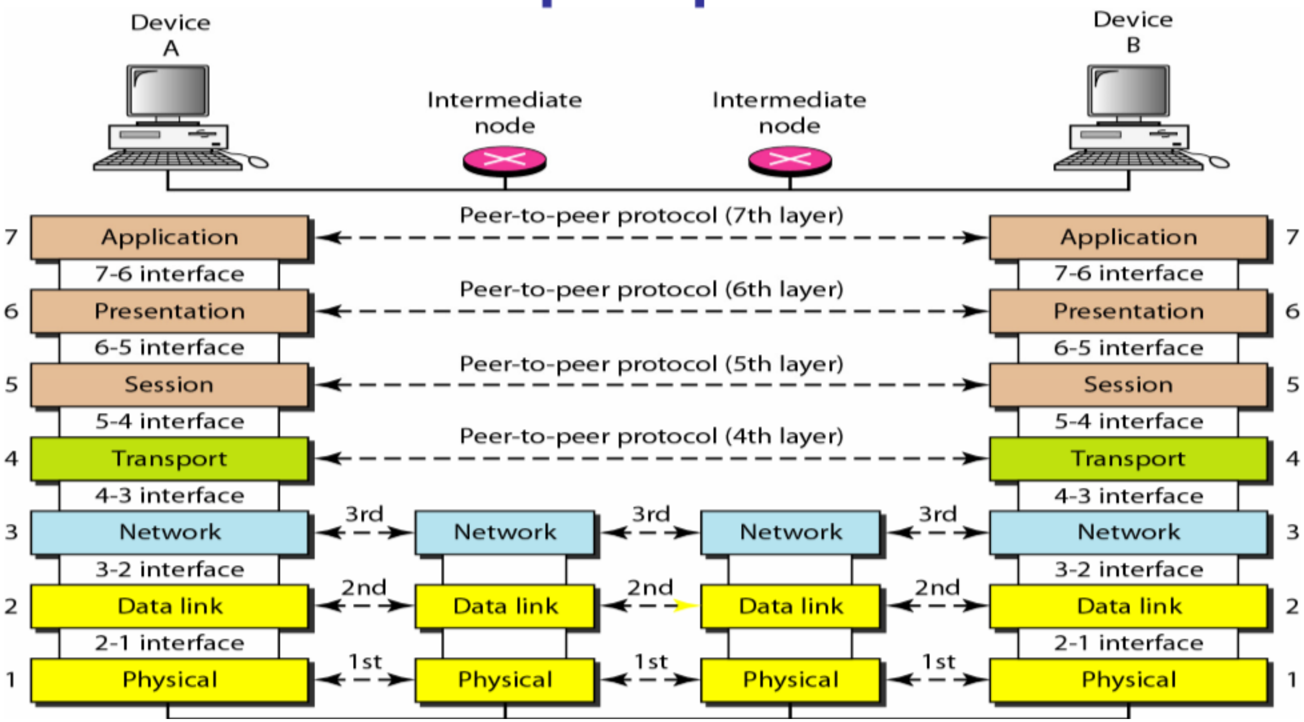
within a single machine, each layer uses the services of the layer below it

between machines, layer *n* on one machine communicates with layer *n* on another machine (as per a protocol) ;

these are called peer-to-peer processes

Network Models & Layered Architecture

Peer-to-peer processes



Network Models & Layered Architecture

Peer-to-peer processes

communication between physical layers is direct, in the form of bit streams

at the higher layers, communication from sender moves down through the layers and then back, up through the layers at the receiver

each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the package to the layer just below it

Network Models & Layered Architecture

Peer-to-peer processes

at layer 1 the entire package is converted to a form transmittable to the receiver

at the receiving system, the message is unwrapped layer by layer

each process receives and removes data meant for it

Network Models & Layered Architecture

Interface between layers

passing of data and network information :

- down, through the layers of sending device
- back up, through the layers of receiving device

is made possible by an interface between each pair of adjacent layers

each interface defines the information and services a layer must provide to the layer above it

well-defined interfaces and layer functions are essential for modularity

Organization of the OSI layers

seven layers, belonging to three subgroups :

- **layers 1, 2, 3 : network support layers** (hardware + software)
- **layer 4 : transport layer** (software)
- **layers 5, 6, 7 : user support layers** (software)

layers 1, 2, 3 :

deal with moving data from one device to another ....

electrical specs, physical connections, physical addressing, timing, reliability

Network Models & Layered Architecture

Organization of the OSI layers

layer 4 :

links the two subgroups viz. network support and user support layers

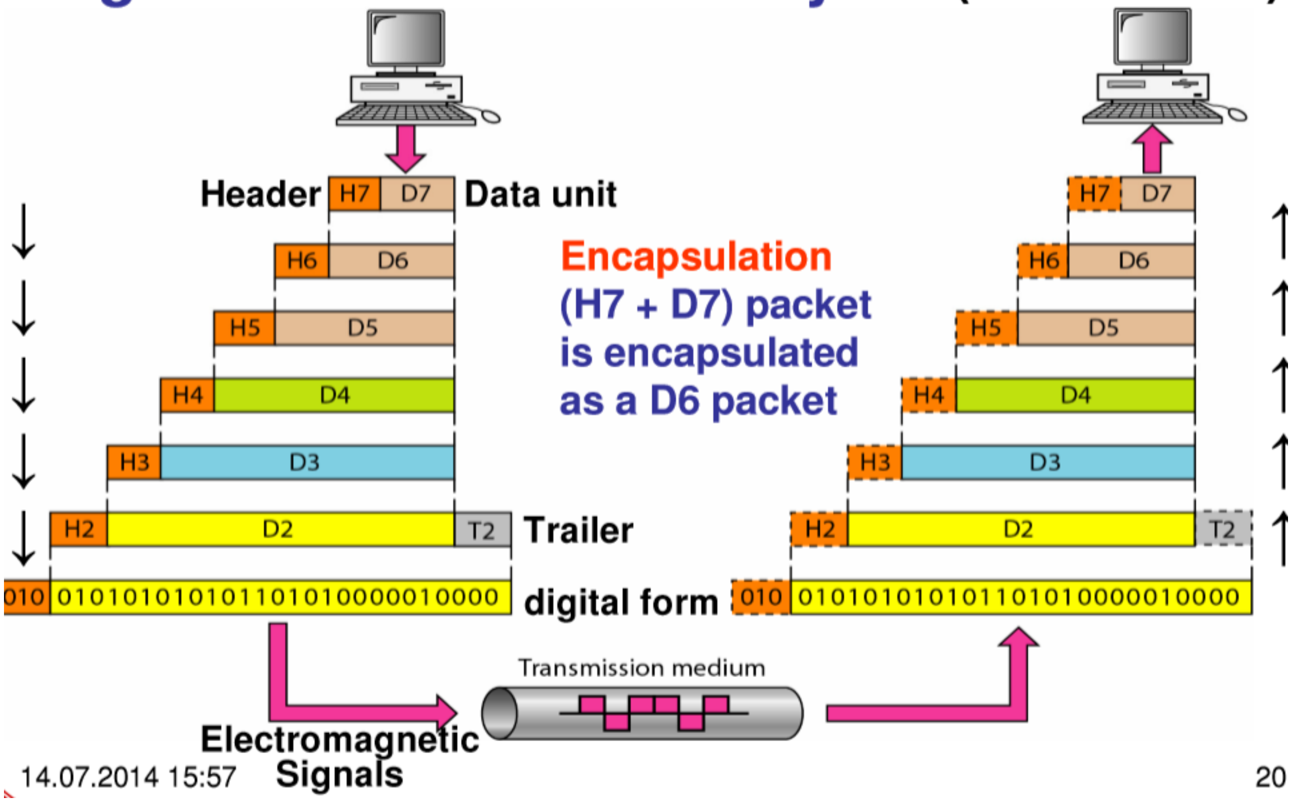
ensures that lower layers transmit entities in a form that the upper layers can make use of

layers 5, 6, 7 :

allow interoperability among unrelated software systems

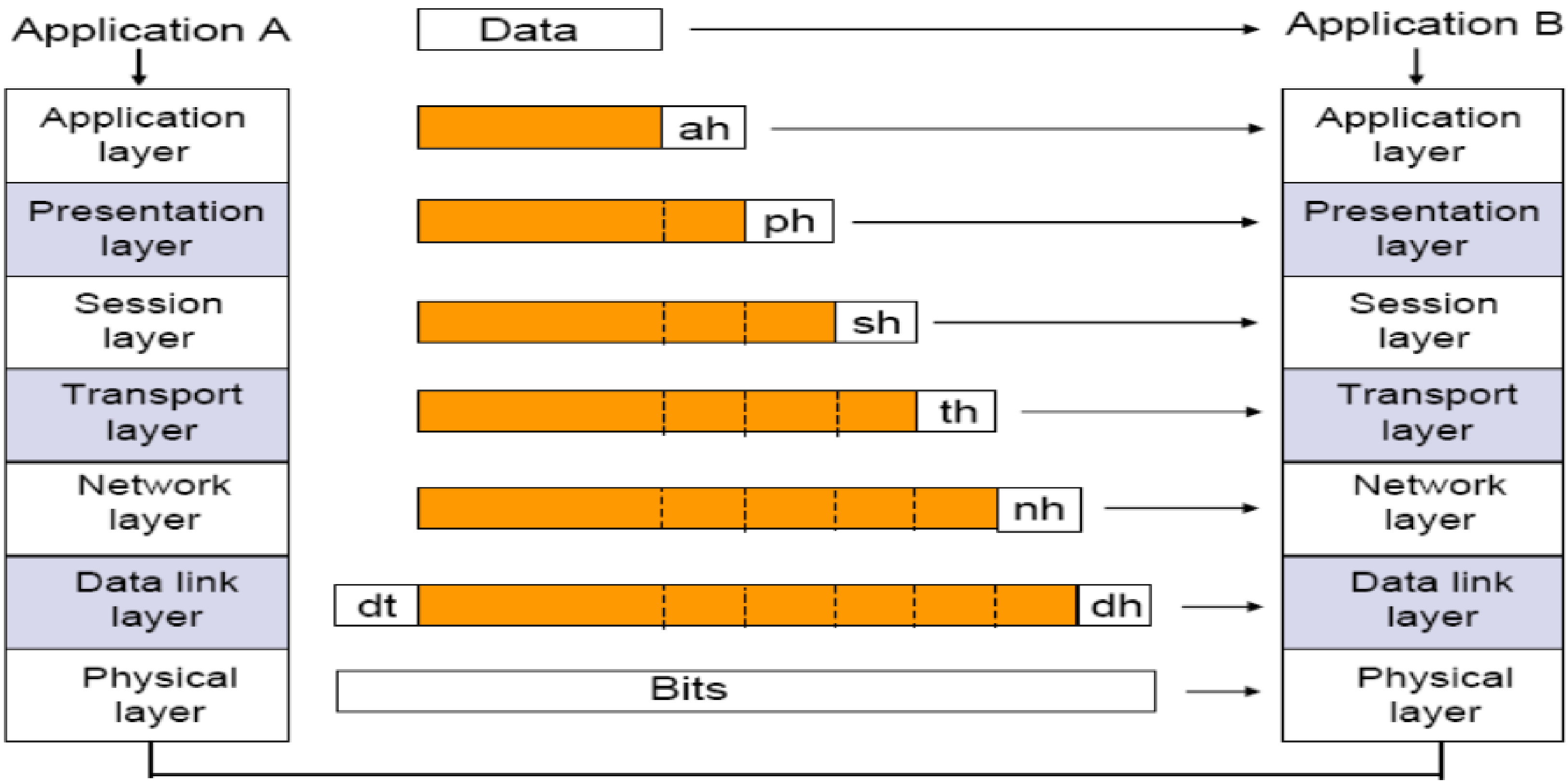
Network Models & Layered Architecture

Organization of the OSI layers (overall view)



Network Models & Layered Architecture

OSI Layers

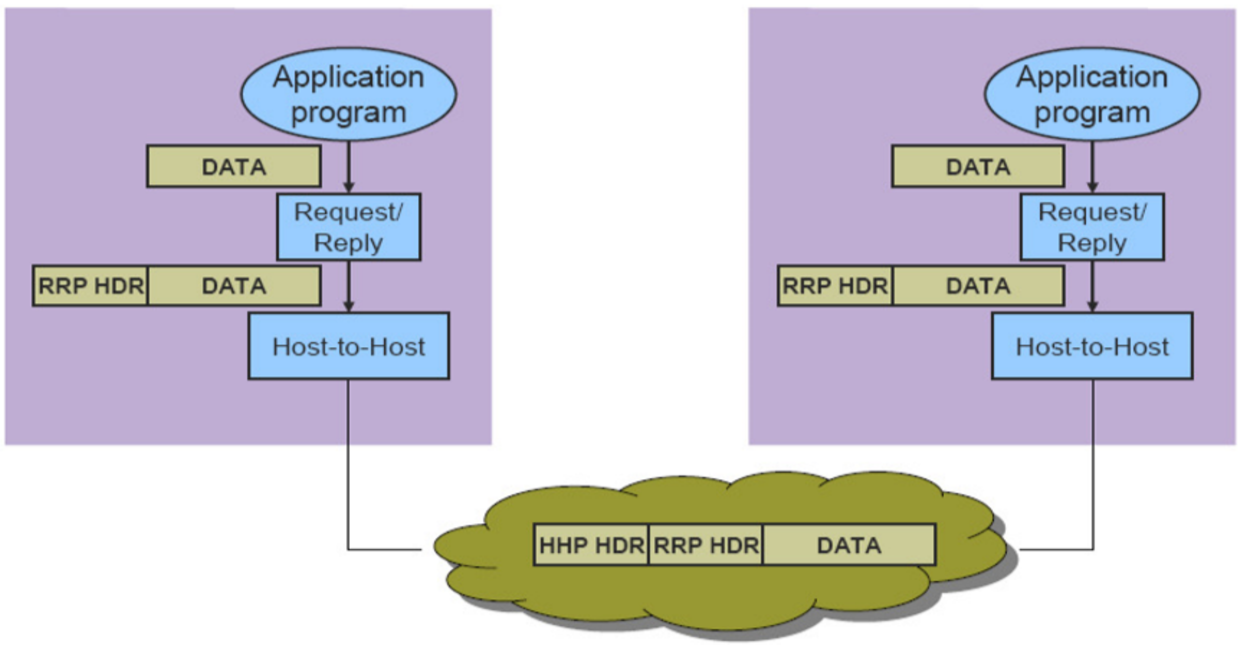


headers and trailers are added to a block of data as it moves down the layers

Network Models & Layered Architecture

Network Architecture

Encapsulation - use of headers and trailers



Network Models & Layered Architecture

Example

TB 1.20

Total no. of header bytes per message

$$= nh$$

The total message size = $(M + nh)$

Fraction of bandwidth occupied by the headers

$$= nh \div (M + nh)$$

Problem-1

- A system has an 5layer protocol hierarchy. App lications generate messages of length 10 bytes . At each of the layers, an 5byte header is add ed. What fraction of the network band-width is filled with headers?

Problem-1

- So total no of header bytes = n*h
- Each message generated is M bytes long.
- So total message size is M+nh
- Fraction of the network bandwidth is filled with headers = Total header size/Total message size =(n*h)/(M+nh)
- if we take no of layer (n)=5
- Message size=10 bytes
- header size =5 bytes
- Total no. header= 5*5=25
- Message size= 10+25=35
-

Network Models & Layered Architecture

OSI layers : Physical layer

responsible for movements of individual *bits* from one hop / node to the next viz.

carries *bit streams* over the physical medium

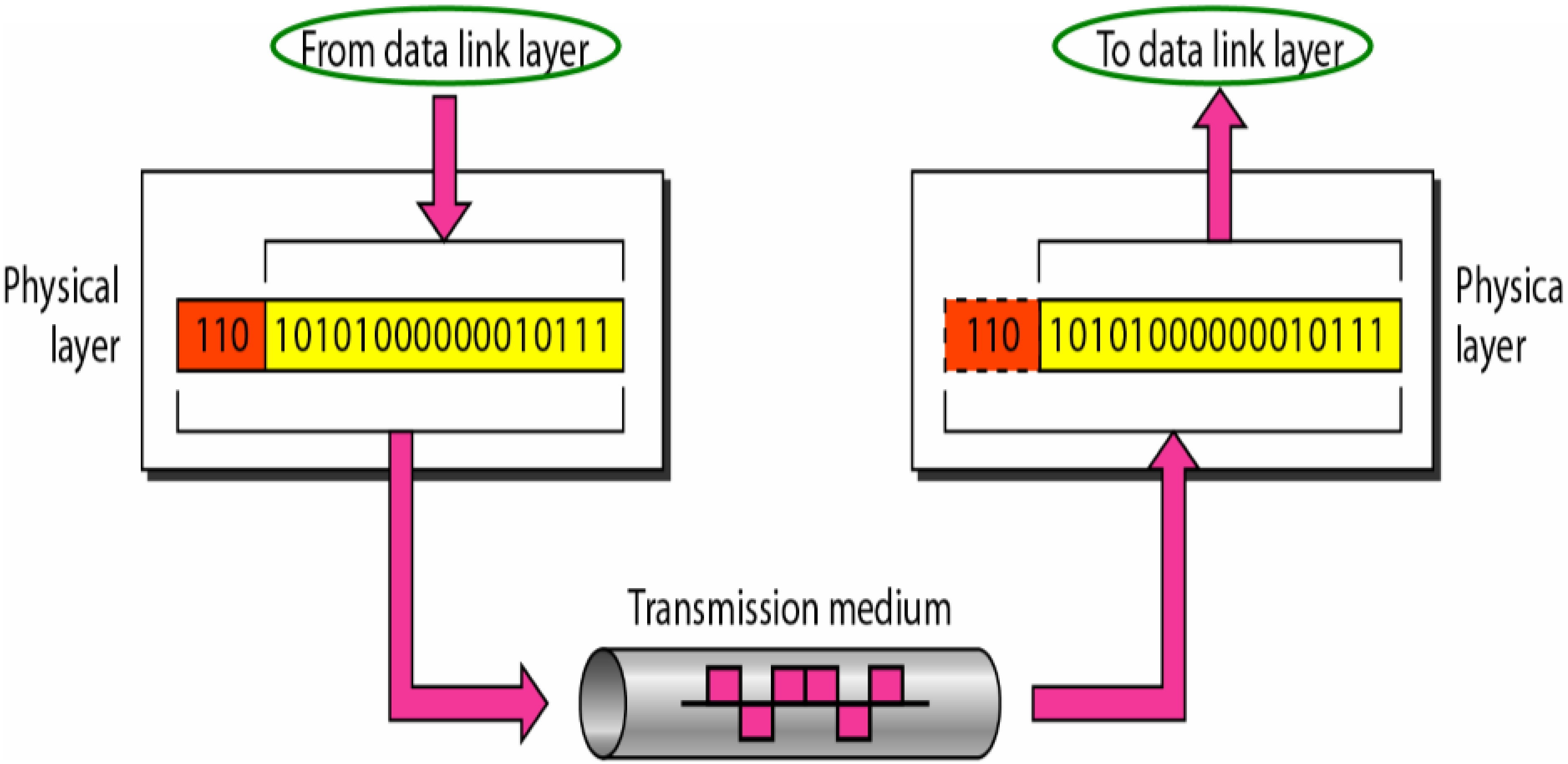
deals with mechanical and electrical specifications of the interface and the transmission medium

defines procedures and functions that physical devices and interfaces have to perform to facilitate transmission

Network Models & Layered Architecture

OSI layers : Physical layer

moves individual *bits* over the medium / link



Network Models & Layered Architecture

OSI layers : Physical layer - tasks

- bit-by-bit delivery
- providing a standardized interface to physical transmission media, including :
  (a) mechanical specification of electrical connectors and cables, for example maximum cable length
  (b) electrical specification of transmission line signal level and impedance

Network Models & Layered Architecture

OSI layers : Physical layer - tasks

(c) radio interface, including .....
electromagnetic spectrum frequency allocation and specification of signal strength, analog bandwidth, etc.

(d) specifications for IR over optical fiber or a wireless IR communication link

- modulation
- line coding
- bit synchronization in synchronous serial communication

Network Models & Layered Architecture

OSI layers : Physical layer - tasks

- start-stop signalling and flow control in asynchronous serial communication
- circuit switching - establishing and termination of connections
- multiplexing
- carrier sense and collision detection utilized by some level 2 MAC protocols
- bit-rate
- point-to-point, multipoint, point-to-multipoint line configuration

Network Models & Layered Architecture

OSI layers : Physical layer - tasks

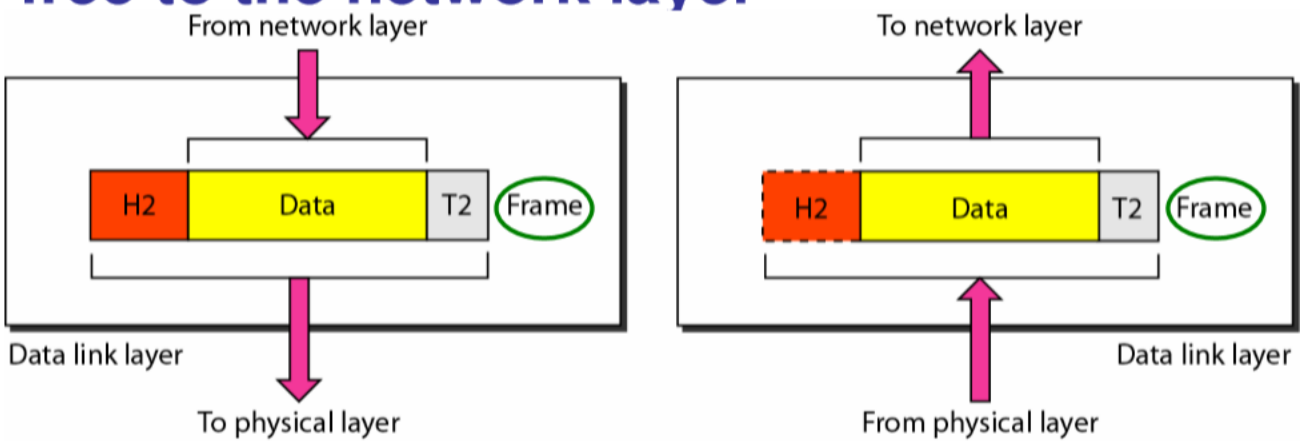
- physical network topology, for example bus, ring, mesh or star network
- serial or parallel communication
- simplex, half-duplex or full-duplex transmission mode
- autonegotiation

Network Models & Layered Architecture

OSI layers : Data Link layer

transforms the physical layer or a raw transmission facility to a *reliable* link

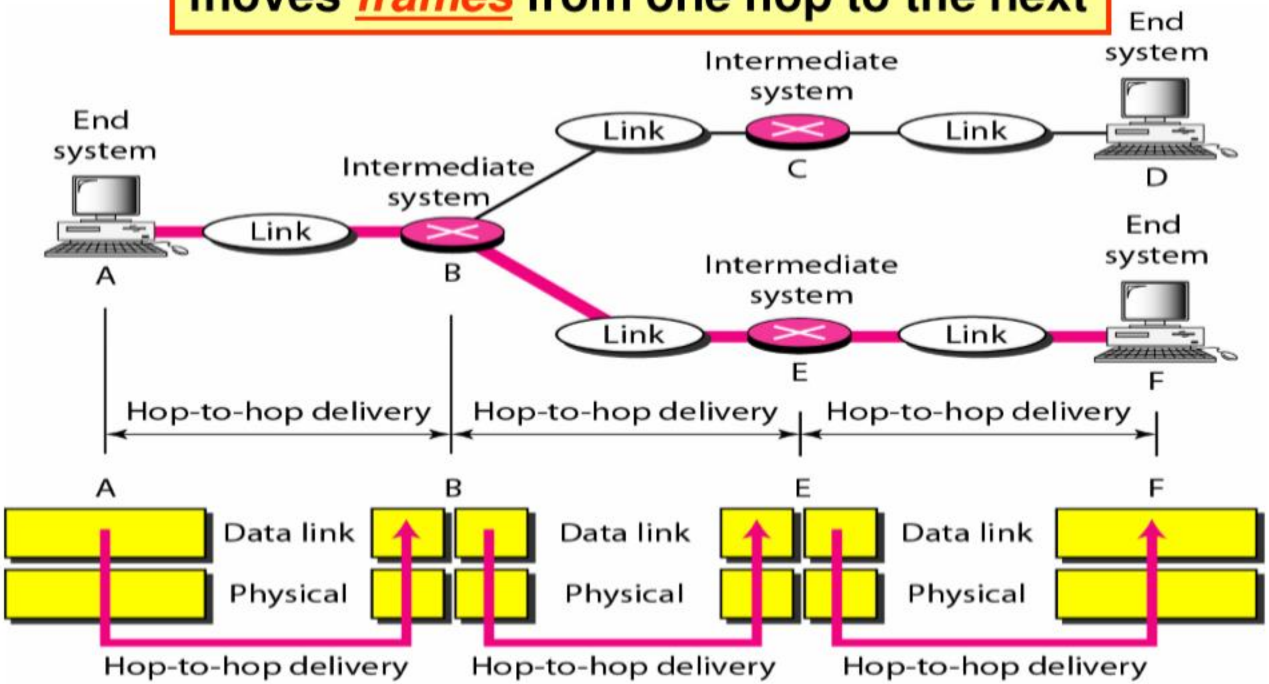
makes the physical layer appear error-free to the network layer



Network Models & Layered Architecture

OSI layers : Data Link layer

moves *frames* from one hop to the next



Network Models & Layered Architecture

OSI layers : Data Link layer - tasks

- framing - dividing stream of bits received from the network layer into manageable data units

- physical addressing - defining the sender and / or receiver

- flow control - preventing sender from overwhelming the receiver

Network Models & Layered Architecture

OSI layers : Data Link layer - tasks

- error control - detecting and retransmitting damaged or lost frames

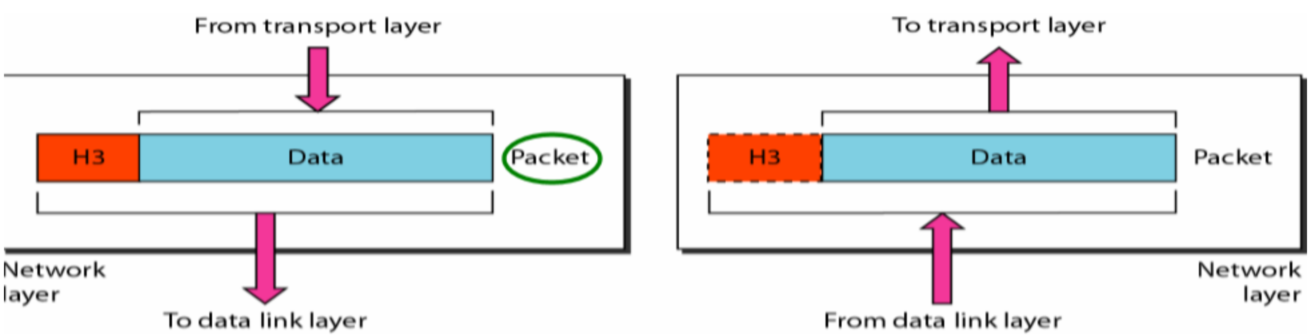
- access control - regulating access to the link when two or more devices are connected

Network Models & Layered Architecture

OSI layers : Network layer

responsible for delivery from source *host* to destination *host*

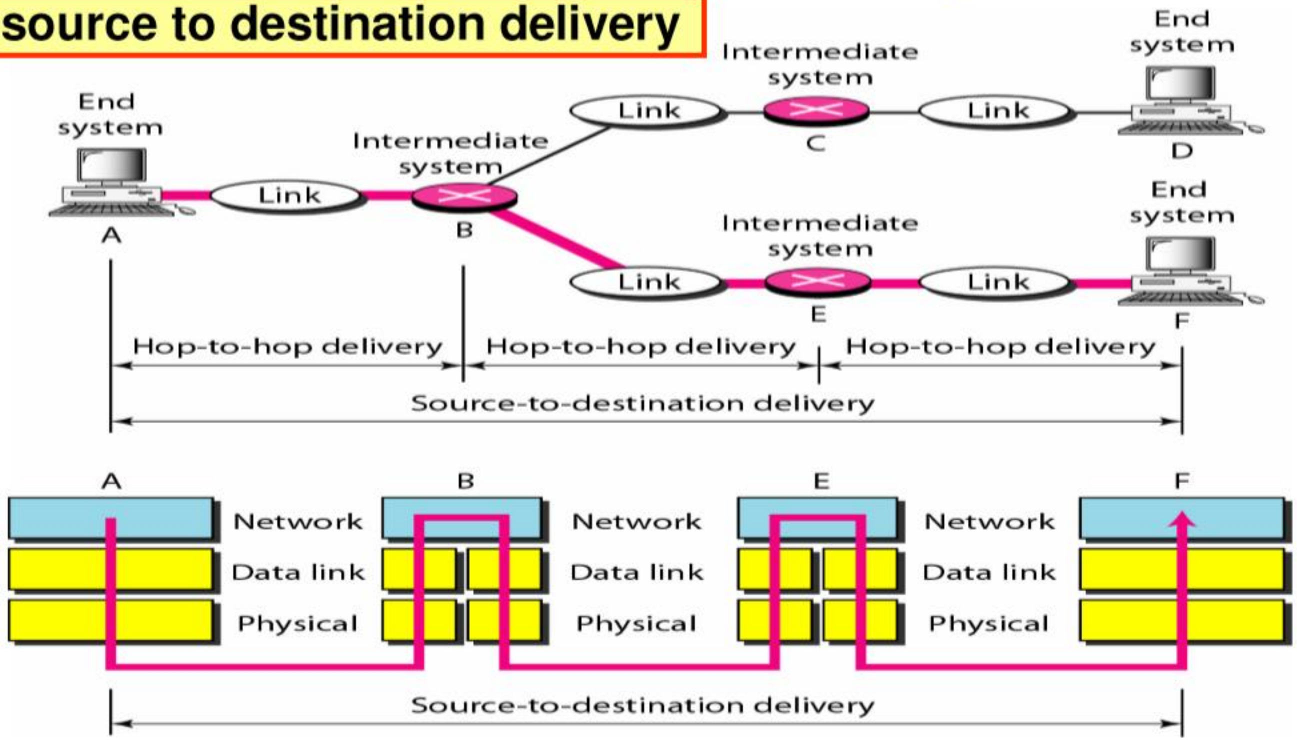
handles delivery of *packet* from its point-of-origin to its final destination possibly across multiple networks



Network Models & Layered Architecture

OSI layers : Network layer

source to destination delivery



Network Models & Layered Architecture

OSI layers : Network layer - tasks

- logical addressing - including logical addresses of the sender and receiver
- routing - sending packets to their final destination through intermediate networks

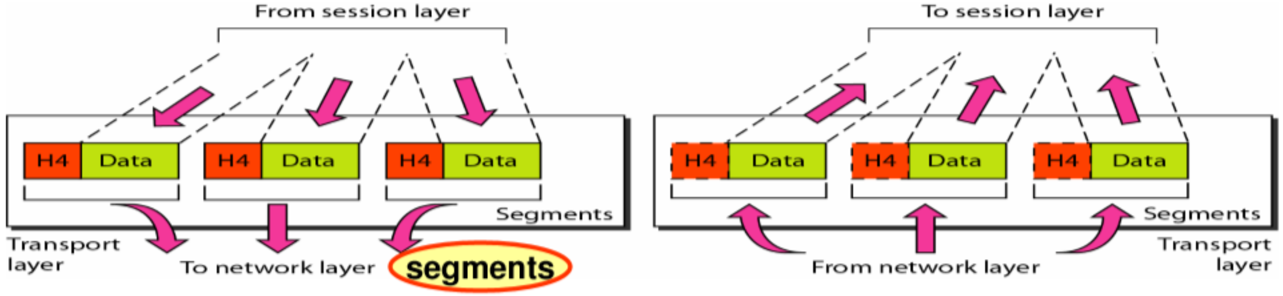
Network Models & Layered Architecture

OSI layers : Transport layer

is responsible for *process - to - process* delivery of the entire *message* (a running program)

ensures that the whole message arrives in tact and in order

oversees both error control and flow control at the source-to-destination level



Network Models & Layered Architecture

OSI layers : Transport layer - tasks

- service-point or port addressing - for delivery from a specific process on one computer to a specific process on another computer

- segmentation and reassembly - for dividing messages into numbered transmittable segments

Network Models & Layered Architecture

OSI layers : Transport layer - tasks

- connection control - for making connection with the transport layer at the destination machine before delivery

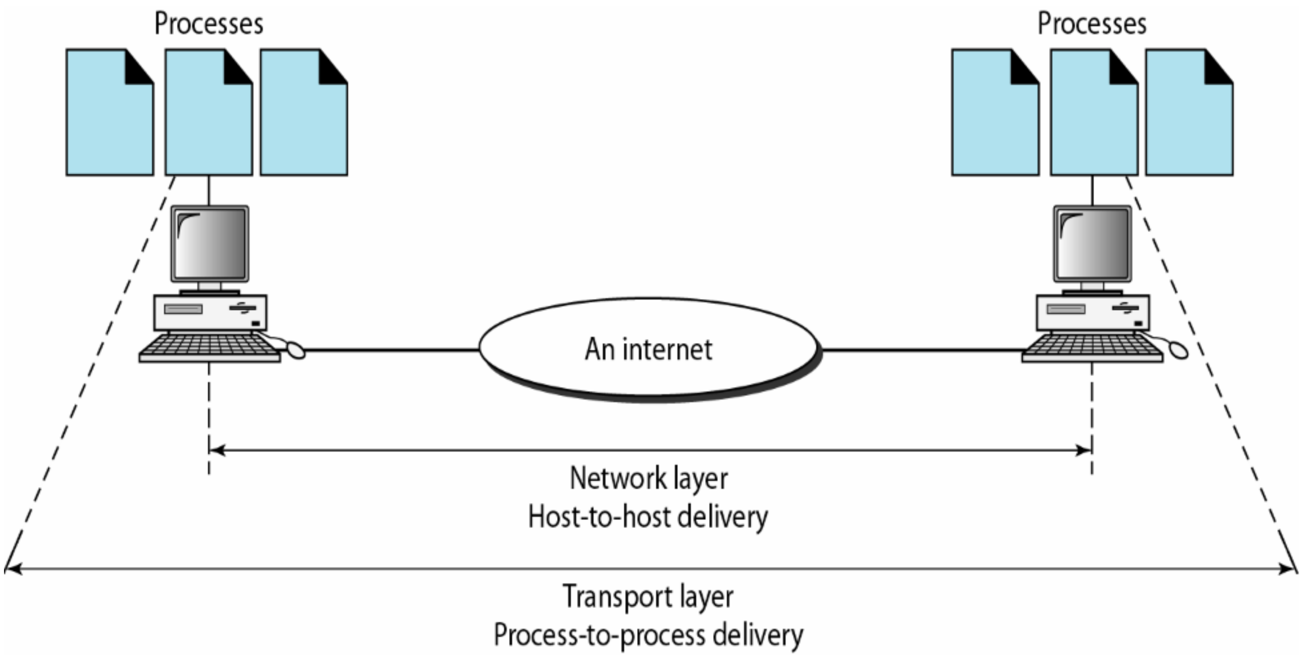
- flow control : end-to-end

- error control : from process-to-process

Network Models & Layered Architecture

OSI layers : Transport layer

reliable process to process delivery



Network Models & Layered Architecture

OSI layers : Session layer

is the network dialog controller

establishes, maintains and synchronizes the interaction among communicating systems

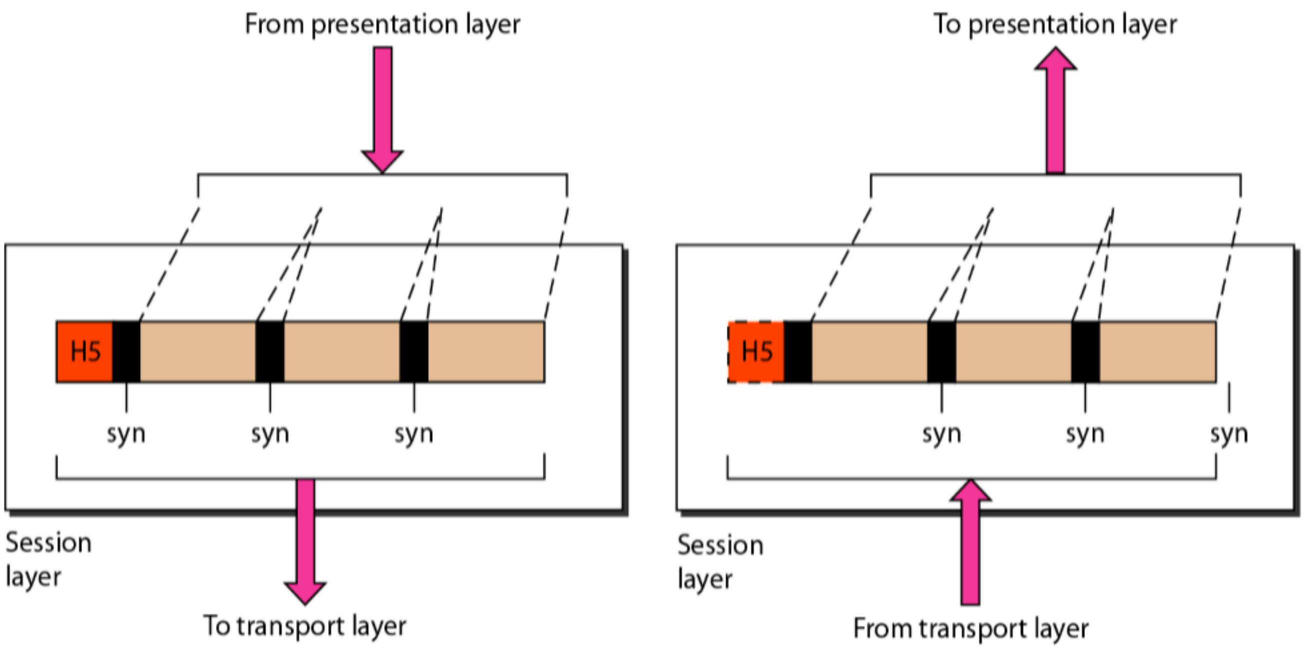
tasks :

- dialog control - allows negotiated mode of communication (half duplex or full duplex) between two processes
- synchronization - allows a process to add check points or synchronization points

Network Models & Layered Architecture

OSI layers : Session layer

dialog control and synchronization



Network Models & Layered Architecture

OSI layers : Presentation layer

concerned with syntax and semantics of the information exchanged between the layers above and below it

tasks :

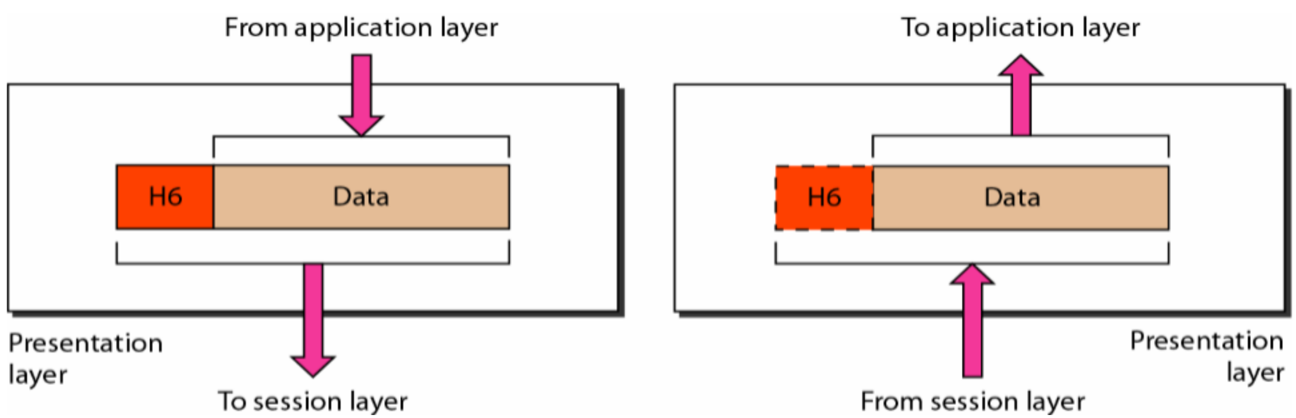
- translation - for achieving .... interoperability between different encoding methods that may be used by different systems by converting sender- dependent or receiver - dependent format to common format

Network Models & Layered Architecture

OSI layers : Presentation layer

tasks : translation, compression, encryption

- encryption - for ensuring privacy
- compression - for reducing the size of transmitted information



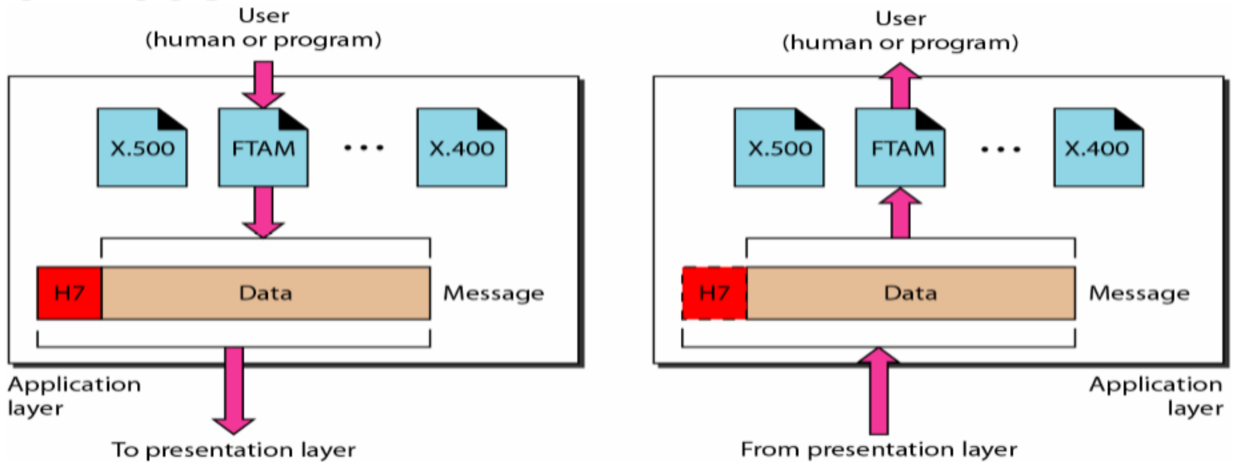
Network Models & Layered Architecture

OSI layers : Application layer

enables the user (human / software) to access the network

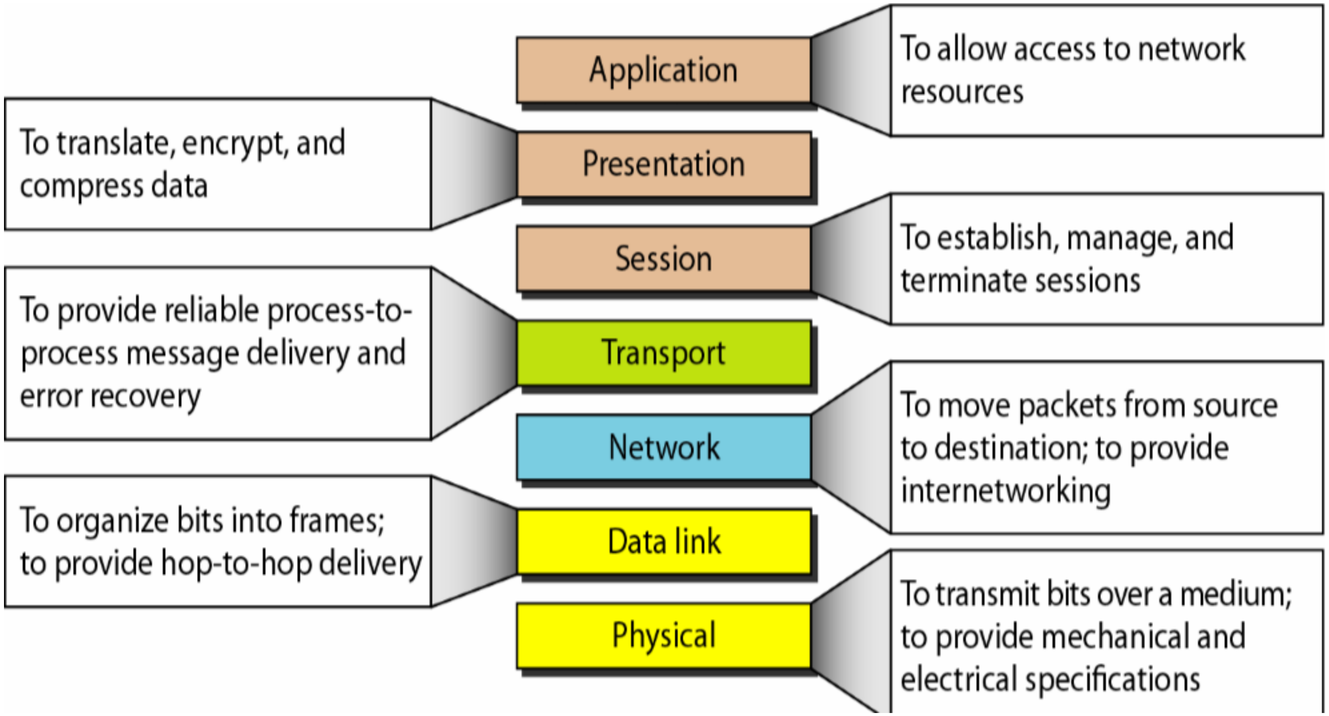
providing service to the user

provides user interfaces and support for services



Network Models & Layered Architecture

OSI layers : Summary



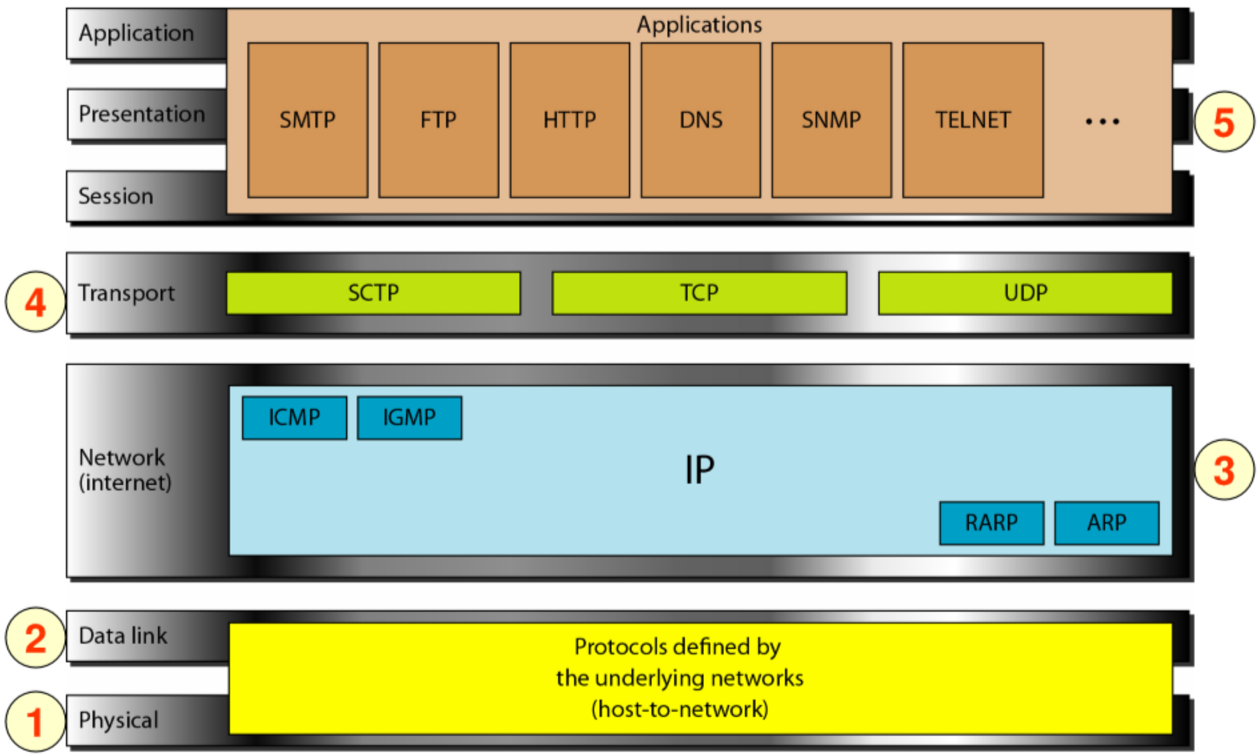
Network Models & Layered Architecture

TCP / IP Protocol Suite : layers

Layer No.	Layer in TCP / IP Protocol suite	Layer(s) in OSI Model
5.	application	application presentation session
4.	transport	transport
3.	internet	network
2. 1.	host-to-network (also called link layer)	data link physical

Network Models & Layered Architecture

TCP / IP Protocol Suite



Network Models & Layered Architecture

TCP / IP Protocol Suite

Physical and Datalink layers :

no specific protocol is defined

supports all standard and proprietary protocols

a network in a TCP/IP internetwork can be a LAN or a WAN

Network Models & Layered Architecture

TCP / IP Protocol Suite

Network Layer :

TCP / IP supports :

- **Internetworking Protocol (IP)**

IP, in turn, uses four supporting protocols :

- **ARP**
- **RARP**
- **ICMP**
- **IGMP**

Network Models & Layered Architecture

TCP / IP Protocol Suite

Network Layer : IP

is the transmission mechanism used by TCP / IP

is an *unreliable* and *connectionless* protocol

provides *best-effort delivery* service, without error checking or tracking or guarantees

transport data in packets called *datagrams*

each datagram is transported separately

Network Models & Layered Architecture

TCP / IP Protocol Suite

Network Layer : IP

datagrams :

- can travel in different routes
- can be duplicated
- can arrive out of sequence
- can be lost

Network Models & Layered Architecture

TCP / IP Protocol Suite

Network Layer :

Address Resolution Protocol (ARP)

used to find the physical address ……

(imprinted on the NIC) of a node ….

on a network (like a LAN) where ……

each device is identified by a logical or IP address

Network Models & Layered Architecture

TCP / IP Protocol Suite

Network Layer :

Reverse Address Resolution Protocol (RARP)

used by a host to discover its IP address when it knows only its physical address

used when the computer is plugged into a network or when it is rebooted

Network Models & Layered Architecture

TCP / IP Protocol Suite

Network Layer :

Internet Control Message Protocol (ICMP)

used by hosts and routers to send …..

notifications (about problems with datagrams) back to the sender of datagrams

query and error reporting messages are sent

Internet Group Message Protocol (IGMP)

used to facilitate simultaneous transmission of a message to a group of recipients

Network Models & Layered Architecture

TCP / IP Protocol Suite

Transport Layer : Protocols

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- Stream Control Transmission Protocol (SCTP)

UDP :

simple protocol

connection-less

has very few header fields

provides limited transport-layer services

Network Models & Layered Architecture

TCP / IP Protocol Suite

Transport Layer : Protocols

TCP :

provides full transport-layer services to applications

is a reliable connection-oriented protocol

divides a stream into segments

each segment includes a sequence number for reordering after receipt and ...

an acknowledgement number for the segments received

Network Models & Layered Architecture

TCP / IP Protocol Suite

Transport Layer : Protocols

SCTP :

provides support for applications such as voice over the Internet (VoIP)

combines the best features of UDP and TCP

Network Models & Layered Architecture

TCP / IP Protocol Suite

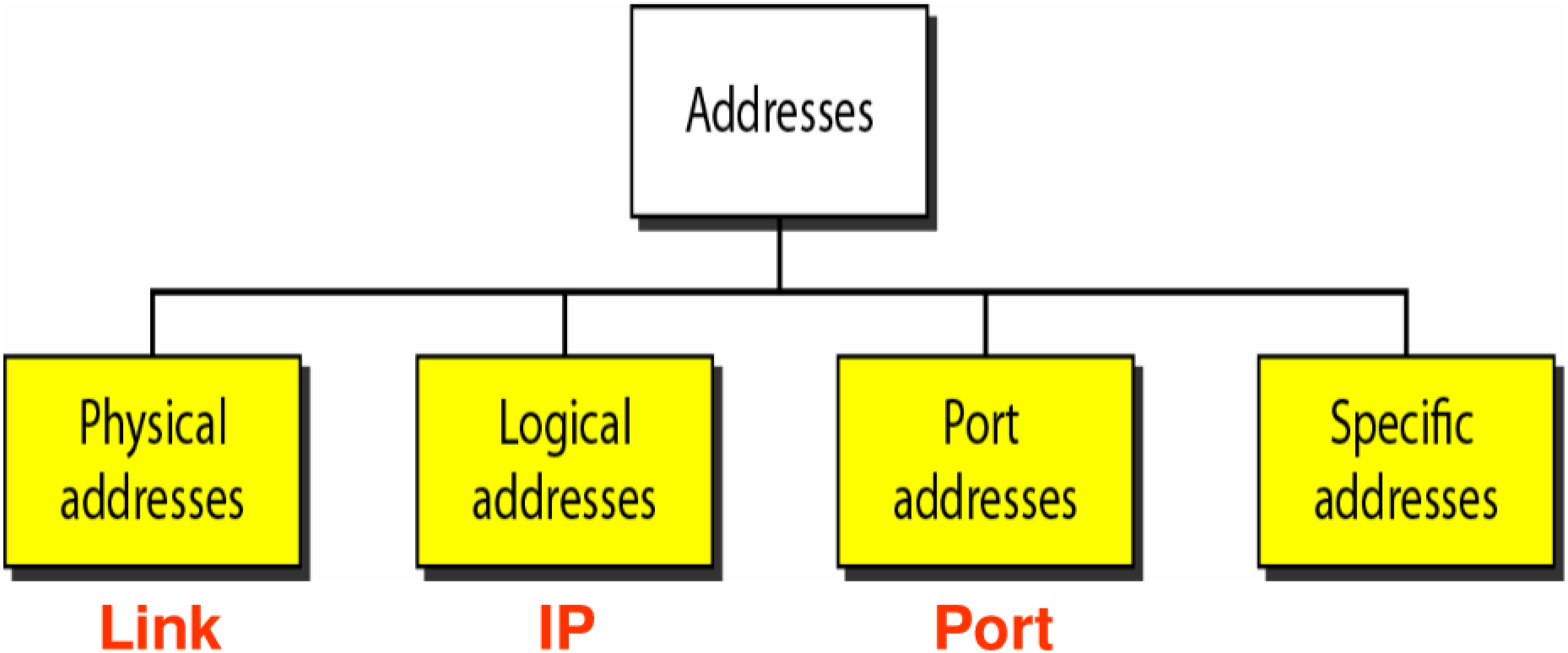
Application Layer

equivalent to the combination of the following layers of the OSI model :

- session
- presentation
- application

Network Models & Layered Architecture

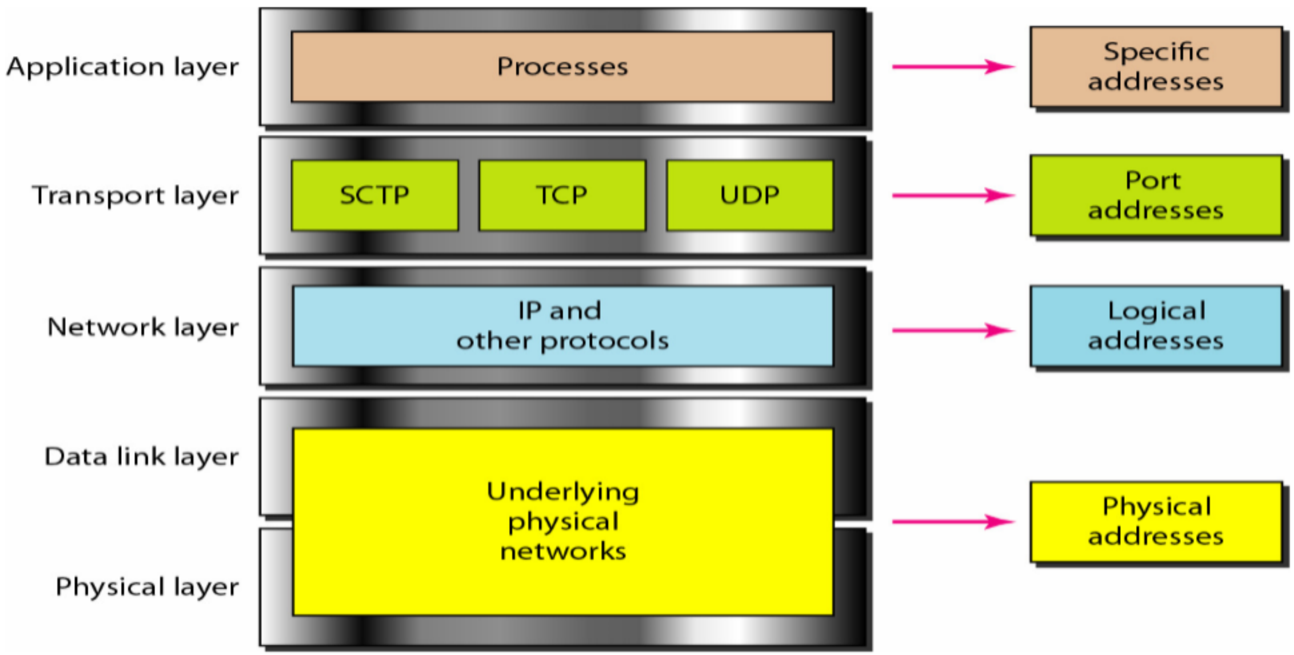
Addressing



Network Models & Layered Architecture

Addressing

Relationship of layers and addresses



Addressing

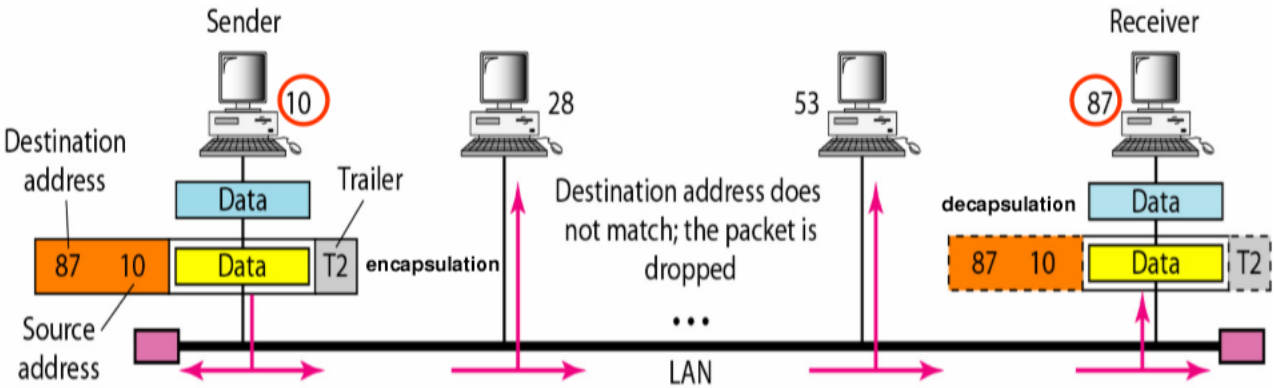
Physical address

also known as the link address
is included in the frame used by ….
the data link layer
is the lowest - level address
size and format can vary depending on the network :
Ethernet : 48-bit physical address imprinted on the NIC
LocalTalk (Apple) : 8-bit dynamic address – changes every time the station is booted

Network Models & Layered Architecture

Addressing

Physical addresses



LAN / physical address : Example

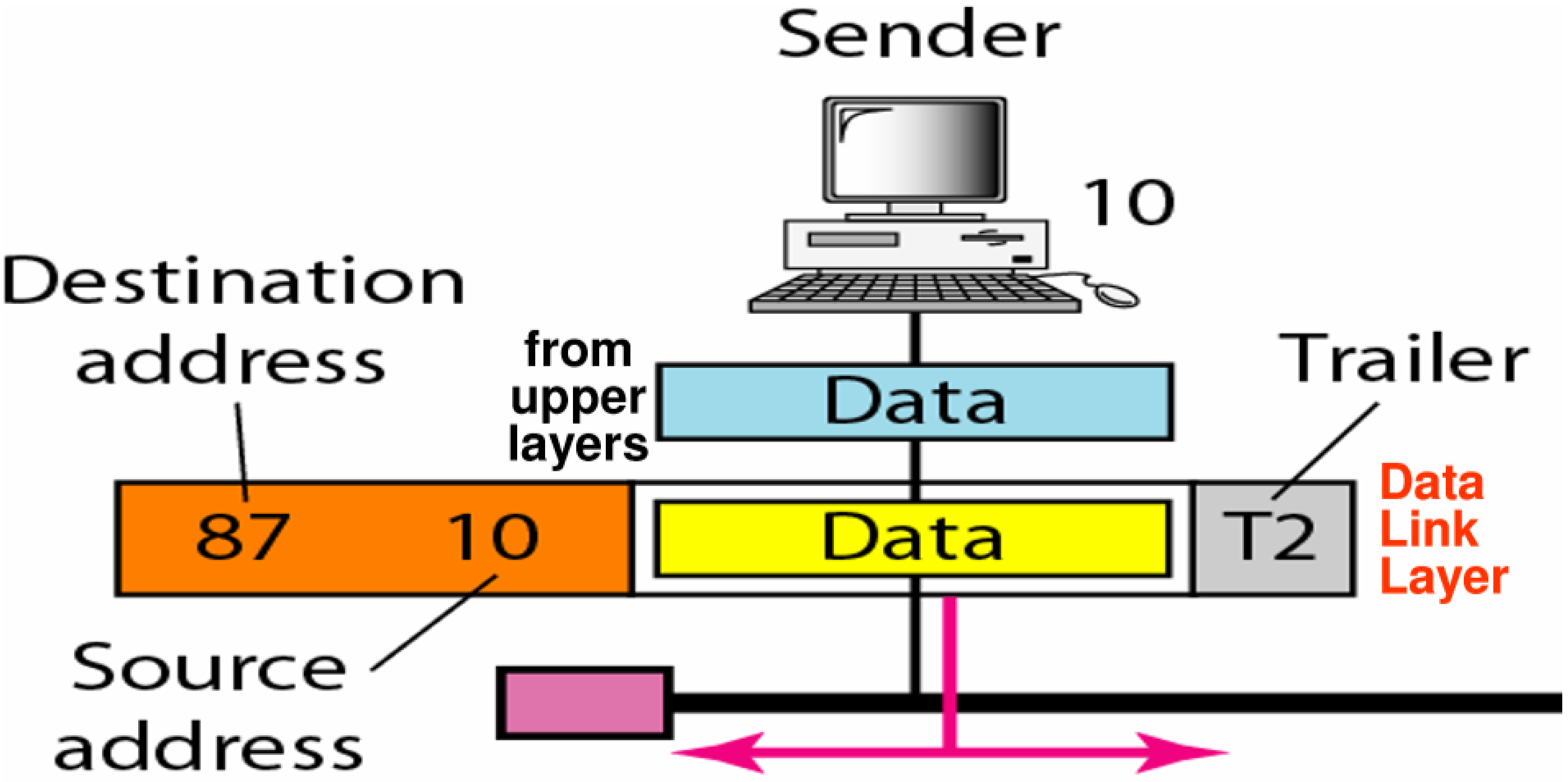
00:1B:11:17:A4:91

A 6-byte (12 hexadecimal digits) physical address

Network Models & Layered Architecture

Addressing

Physical address

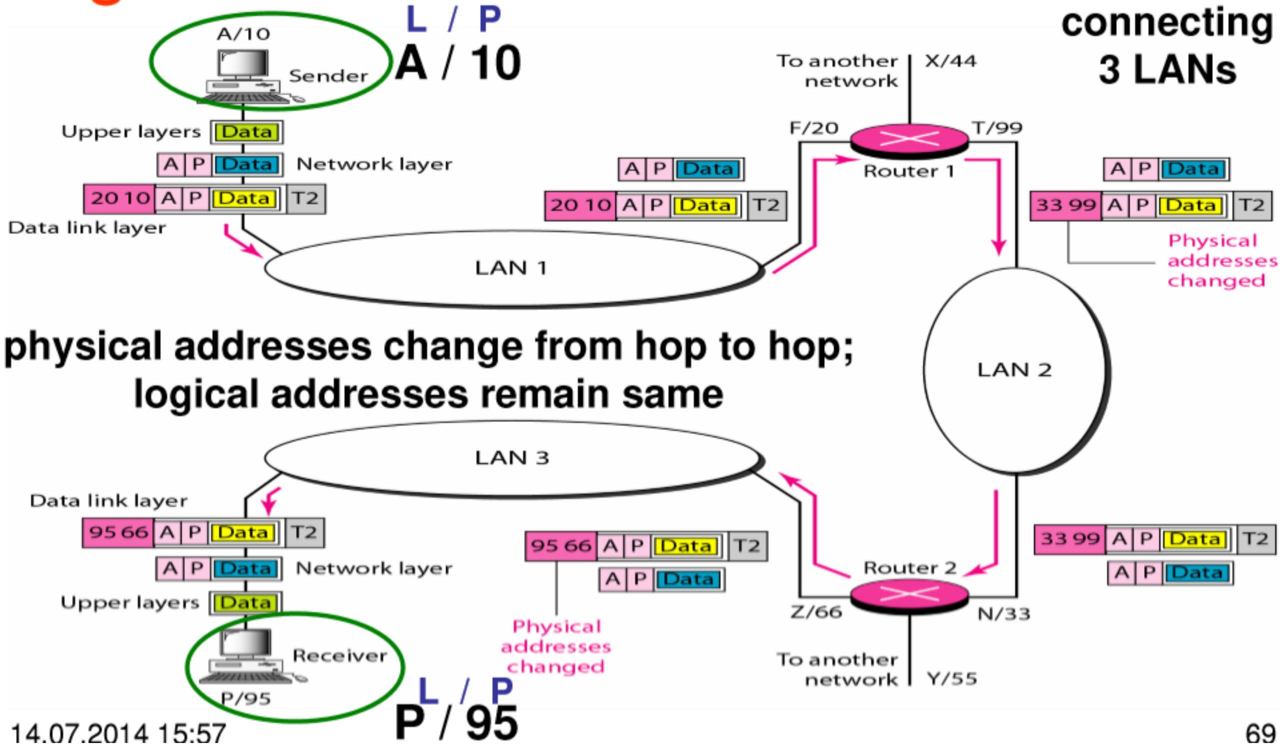


Network Models & Layered Architecture

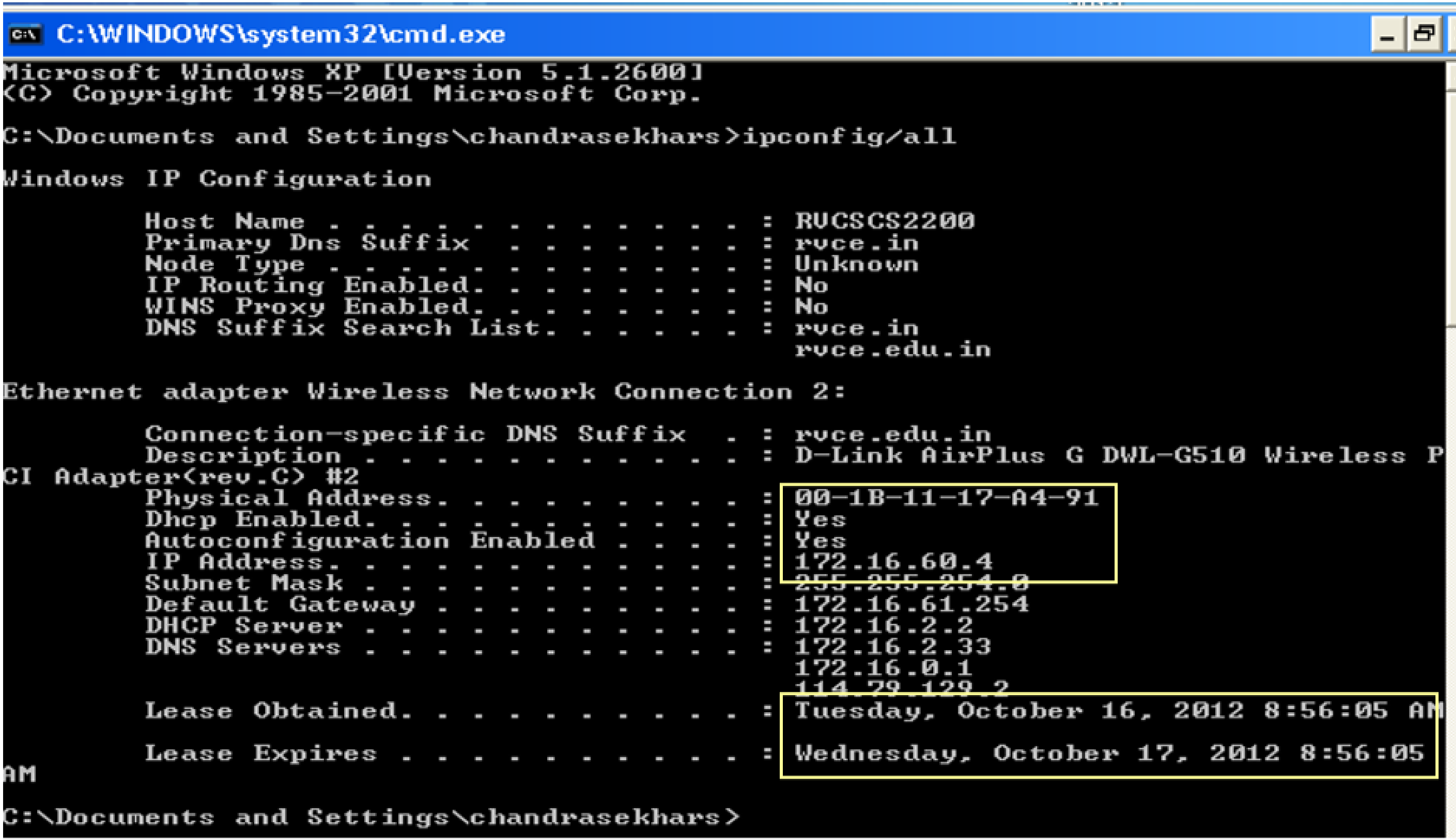
Addressing

Logical addresses

Example of an internet : 2 Routers connecting 3 LANs



physical addresses change from hop to hop; logical addresses remain same



C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\chandrasekhars>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : RVCSCS2200
        Primary Dns Suffix  . . . . . . . : rvce.in
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : rvce.in
                                            rvce.edu.in

Ethernet adapter Wireless Network Connection 2:

        Connection-specific DNS Suffix  . : rvce.edu.in
        Description . . . . . . . . . . . : D-Link AirPlus G DWL-G510 Wireless P
CI Adapter(rev.C) #2
        Physical Address. . . . . . . . . : 00-1B-11-17-A4-91
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.60.4
        Subnet Mask . . . . . . . . . . . : 255.255.254.0
        Default Gateway . . . . . . . . . : 172.16.61.254
        DHCP Server . . . . . . . . . . . : 172.16.2.2
        DNS Servers . . . . . . . . . . . : 172.16.2.33
                                            172.16.0.1
                                            114.79.129.2
        Lease Obtained. . . . . . . . . . : Tuesday, October 16, 2012 8:56:05 AM

        Lease Expires . . . . . . . . . . : Wednesday, October 17, 2012 8:56:05
AM

C:\Documents and Settings\chandrasekhars>
```

Network Models & Layered Architecture

Addressing

Physical address

```
C:\WINDOWS\system32\cmd.exe
icrosoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

:\Documents and Settings\chandrasekhars>ipconfig/all

indows IP Configuration

        Host Name . . . . . . . . . . . . : RVCSCS2200
        Primary Dns Suffix  . . . . . . . : rvce.in
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : rvce.in
                                            rvce.edu.in

thernet adapter Wireless Network Connection 2:

        Connection-specific DNS Suffix  . : rvce.edu.in
        Description . . . . . . . . . . . : D-Link AirPlus G DWL-G510 Wireless P
I Adapter(rev.C) #2
        Physical Address. . . . . . . . . : 00-1B-11-17-A4-91
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.60.8
        Subnet Mask . . . . . . . . . . . : 255.255.254.0
        Default Gateway . . . . . . . . . : 172.16.61.254
        DHCP Server . . . . . . . . . . . : 172.16.2.2
        DNS Servers . . . . . . . . . . . : 172.16.2.33
                                            172.16.0.1
                                            114.79.129.2
        Lease Obtained. . . . . . . . . . : Tuesday, October 30, 2012 9:10:42 AM

        Lease Expires . . . . . . . . . . : Wednesday, October 31, 2012 9:10:42
M

:\Documents and Settings\chandrasekhars>_
```

Network Models & Layered Architecture

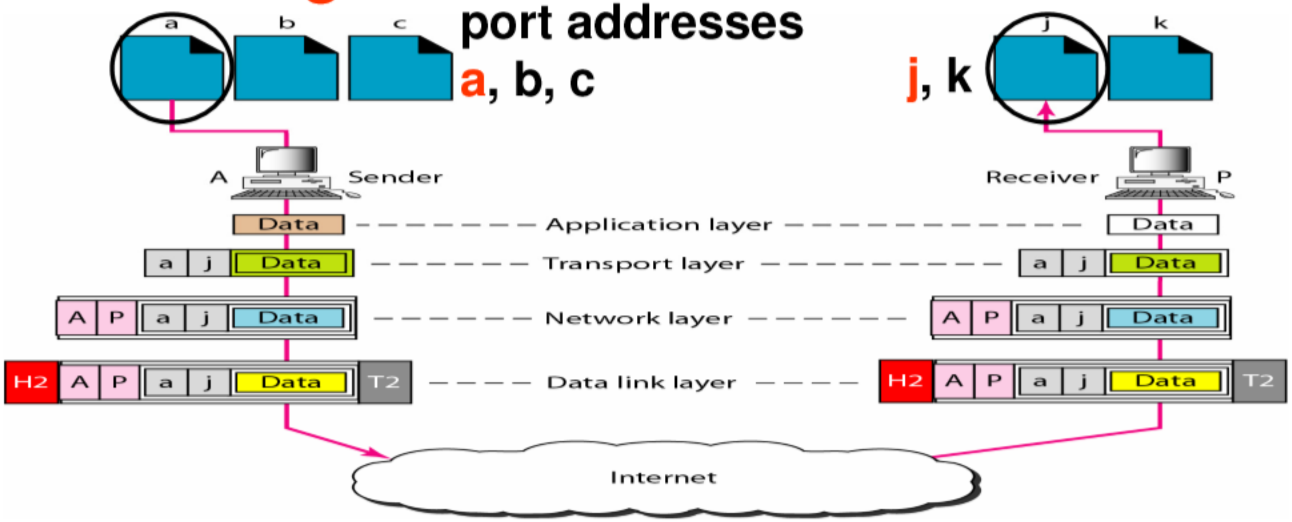
Addressing

Port addresses

physical addresses change from hop to hop; logical and port addresses remain same

a method to label the different processes

16-bit long



 from port a on sender (A) to port j on the receiver (P)

Network Models & Layered Architecture

Addressing

Specific addresses

user-friendly addresses

get changed to corresponding port and logical addresses

Examples:

e-mail address (user1@rvce.edu.in)

Uniform Resource Locator (URL) (www.rvce.edu.in)

Network Models & Layered Architecture

Addressing

Specific addresses

user-friendly addresses

get changed to corresponding port and logical addresses

Examples:

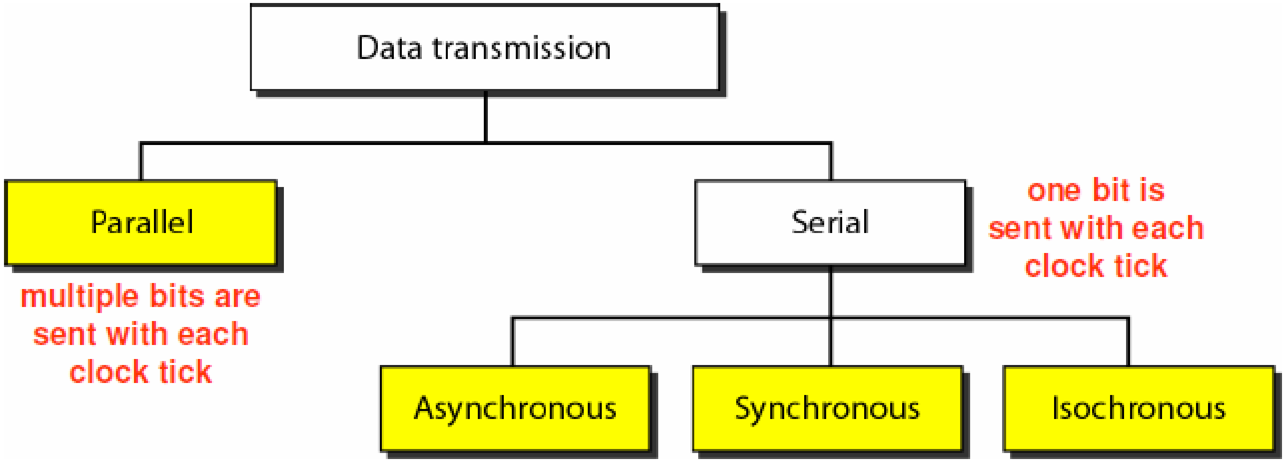
e-mail address (user1@rvce.edu.in)

Uniform Resource Locator (URL) (www.rvce.edu.in)

Digital Transmission

Transmission Modes

used for sending streams of data containing 0s and 1s from one device to another over wire or wires

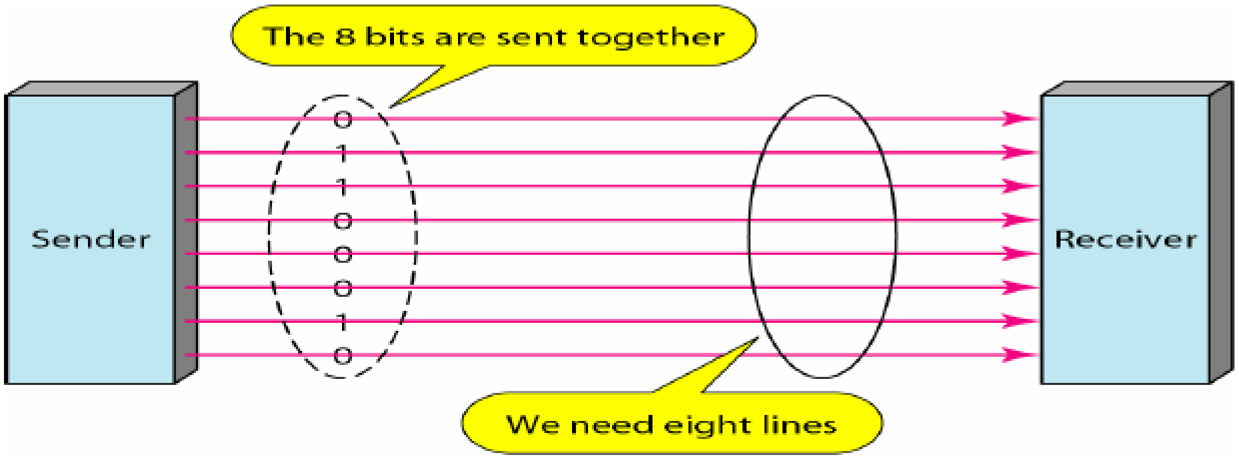


Digital Transmission

Transmission Modes : Parallel

binary data is organized into groups of n bits each and sent at a time

requires use of n wires



Digital Transmission
Transmission Modes : Parallel

advantage :
speed … transfer speed can be increased by a factor of n over the serial method

disadvantage :
cost of communication lines / wires

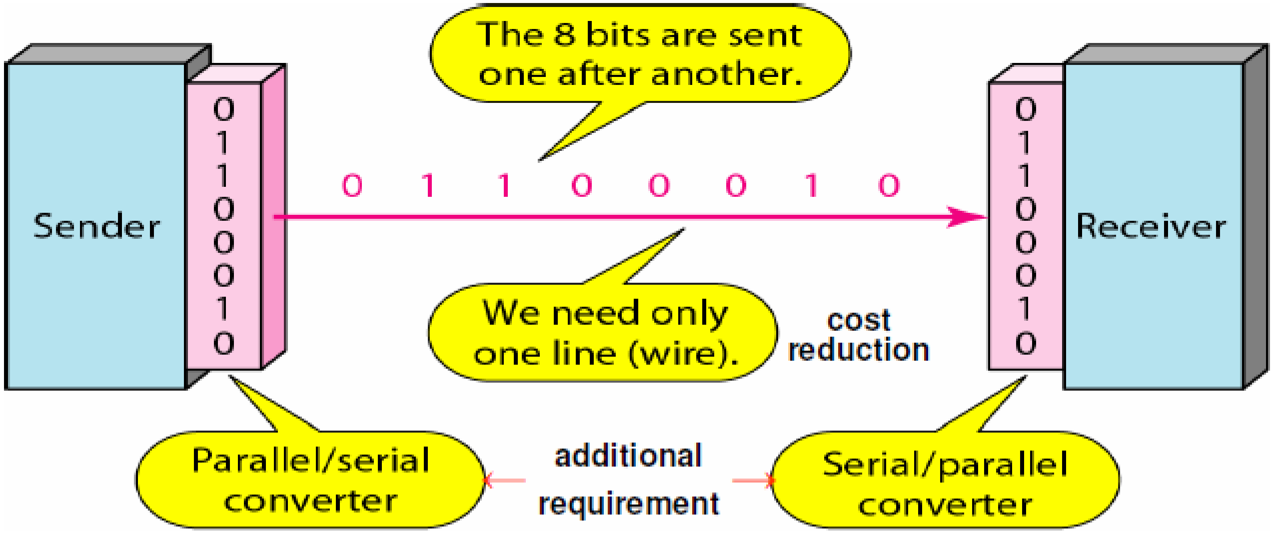
usually limited to short distances

Digital Transmission

Transmission Modes : Serial

one bit follows another

only one communication channel required



Digital Transmission

Transmission Modes : Serial

Asynchronous transmission

the timing of a signal is not important

information is received and translated by agreed upon patterns

by following this pattern, the receiver can retrieve the information

patterns are based on grouping the bit stream into bytes

each group, usually 8 bits, is sent along the link as a unit and handled independently

Digital Transmission

Transmission Modes : Serial

Asynchronous transmission

the start & stop bits and the gap alert the receiver to the beginning and end of each byte

receiving device synchronizes at the onset of each new byte

when the receiver detects a start bit, it sets a timer and begins counting bits as they come in

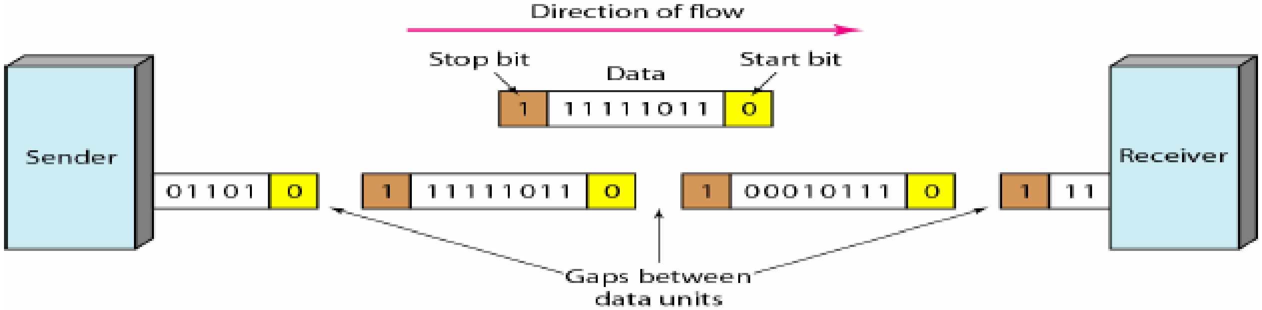
after n (say, 8) bits, the receiver looks for the stop bit

example : keyboard to computer communication

Digital Transmission

Transmission Modes : Serial

Asynchronous transmission



asynchronous at the byte level

but, within each byte, the receiver must be synchronized with the incoming bit stream

advantage : easy to implement, inexpensive

disadvantage : slower, due to overheads

Digital Transmission

Transmission Modes : Serial

Synchronous transmission

bit stream is combined into longer “frames”, containing multiple bytes

transmitted as unbroken strings of 1s and 0s

receiver needs to separate the bit stream into bytes for decoding by counting bits as they arrive and groups them into 8-bit units

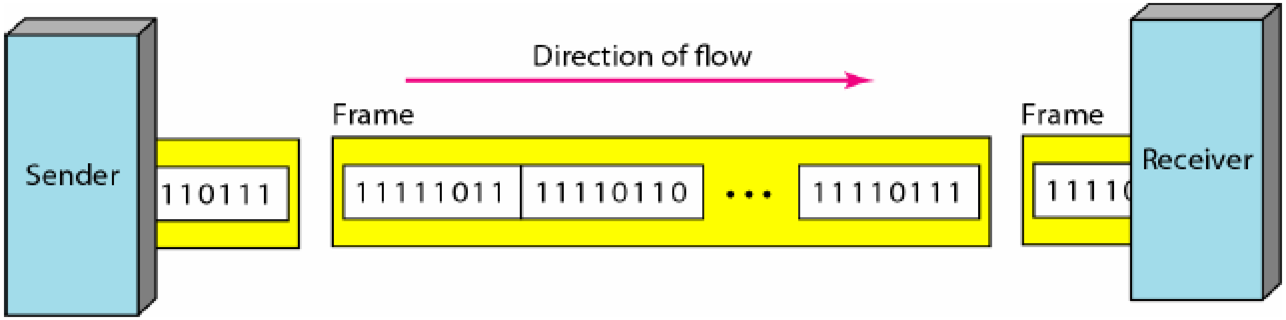
timing is very important :

accuracy of the received information is completely dependent on the ability of the receiver to keep an accurate count of bits as they are received

Digital Transmission

Transmission Modes : Serial

Synchronous transmission



advantage : speed

issue : byte synchronization

Digital Transmission

Transmission Modes : Serial

Isochronous transmission

in real-time audio / video, uneven delays between frames is unacceptable

synchronization between characters is inadequate

synchronization of the entire stream is necessary

isochronous transmission ensures that the data arrive at a fixed rate

Data Link Control

two functions of data link layer :

- data link control
- media access control (how to share the link)

data link control deals with …..
the design and procedures for ……
communication between adjacent nodes
i.e. node-to-node communication

Data Link Control

data link control functions :

- framing
- flow and error control
- software implementation of protocols for smooth and reliable transmission of frames between nodes

implementation of data link control …….
requires protocols run by the two nodes that are….
involved in exchange of data at the data link layer

Data Link Control

Framing

data transmission in physical layer involves synchronized movement of bits in the form of signals from source to destination

in data link layer, bits are packed into *frames*, so that each frame is distinguishable from one another

Data Link Control

Framing

framing in the data link layer ….

separates a message from one source to a destination or from other messages to other destinations

framing is done by adding a sender address and a destination address :

- destination address : for delivery
- sender address : for acknowledgement

message is generally divided into …..

smaller, manageable sized frames

Data Link Control

Framing

- fixed - size framing
- variable - size framing

Variable size framing protocols

- character - oriented protocols
- bit - oriented protocols

Data Link Control

Framing

Fixed - size framing

frame sizes are fixed → no need for defining the boundaries of frames

the size of the frame itself can be used as a delimiter

Example :

Asynchronous Transfer Mode (ATM),

a network technology, which uses a cell of fixed size : 53 bytes, including 48 bytes of data and 5 bytes of header

Data Link Control

Framing

Variable - size framing

used in LANs

requirement :

a method to define the end of a frame and the beginning of the next

two approaches :

- character - oriented protocols
- bit - oriented protocols

Data Link Control

Framing

Character - oriented Protocols

generally used for carrying data comprising 8-bit characters, such as ASCII

consists of 8-bits or multiples of 8-bits :

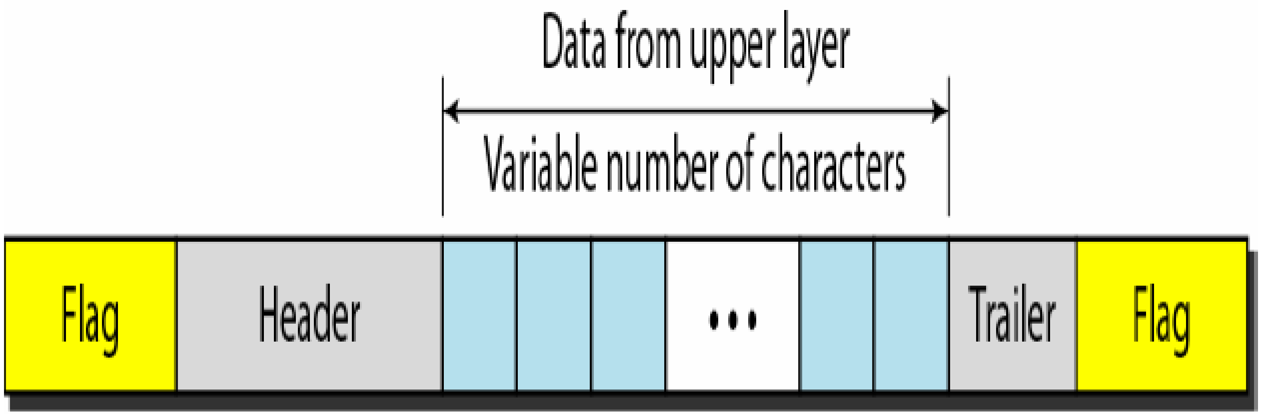
- *header* : carries source and destination address and other control information
- *trailer* : error detection / correction redundant bits
- *flag* : added at the beginning and the end of a frame, to separate one frame from the next

Data Link Control

Framing

Character - oriented Protocols

Frame structure



flag is composed of ***protocol-dependent pattern of special characters*** (1 byte or 8-bit)

Data Link Control

Framing

Character - oriented Protocols

Frame structure : byte stuffing

what happens if the pattern used for the flag also appears as part of data section ?

the receiver, when it encounters the pattern of flag in the middle of data, thinks (erroneously) that it has reached the end of frame

to solve the above, *byte - stuffing* is used in character- oriented framing

also called *character - stuffing*

Data Link Control

Framing

Character - oriented Protocols

Frame structure : byte stuffing

the data section is stuffed with an extra byte, by the sender, whenever a character with the same pattern as the flag is encountered as part of data

this stuffed byte is called the escape character (ESC), which has a pre - defined bit pattern (00011011 or x1B or 27)

Data Link Control

Framing

Character - oriented Protocols

Frame structure : byte stuffing

when the receiver encounters the ESC character ….

the receiver removes the ESC character from the data section and …

treats the flag as data and not a delimiting flag byte

what happens if the data section contains one or more ESC characters followed by a flag ?

→ →

Data Link Control

Framing

Character - oriented Protocols

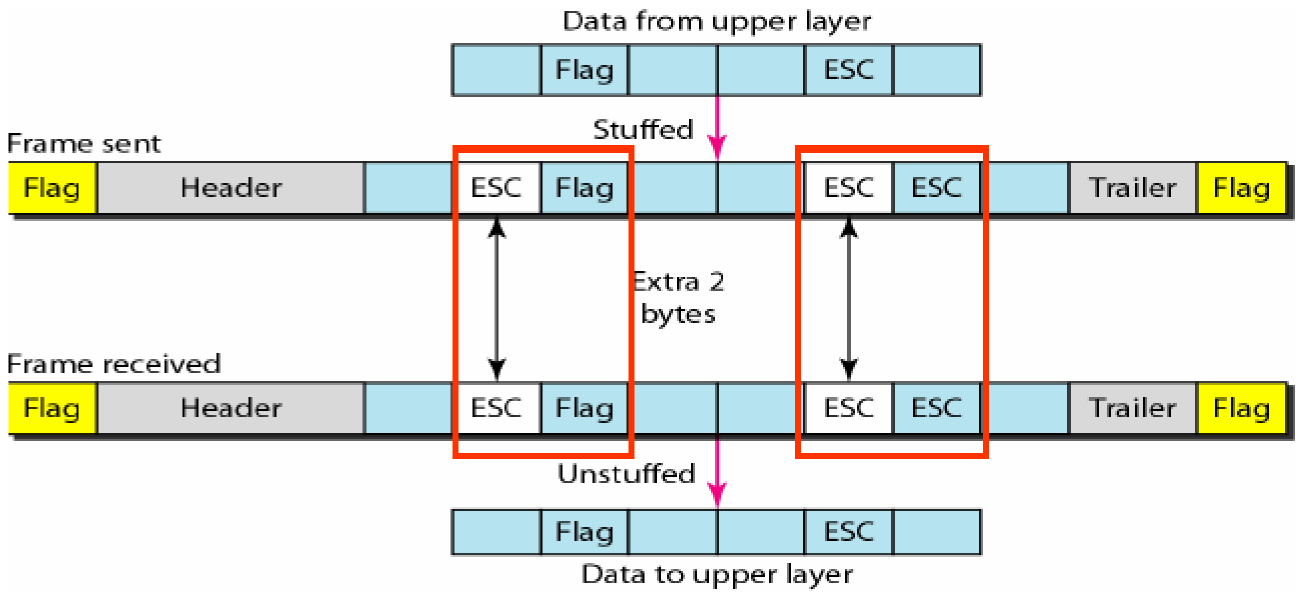
Frame structure : byte stuffing

receiver removes the ESC character, but keeps the flag, which is incorrectly interpreted as end of frame

to solve the above, the ESC characters which are part of data, are also marked by another (extra) ESC character

Byte stuffing involves adding one extra byte (ESC) whenever there is a flag or escape character in the text

Data Link Control
Framing
Character - oriented Protocols
Frame structure : byte stuffing



Data Link Control

Framing

Character - oriented Protocols

Byte stuffing : Example

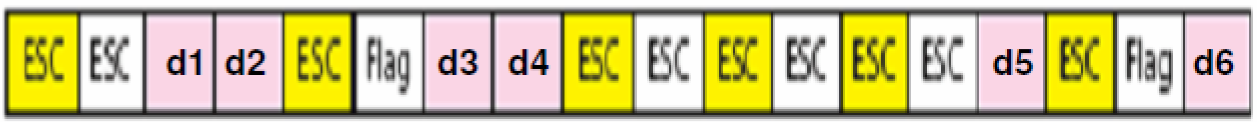
BF4e11.11.13

Byte - stuff the data in the figure below.

ESC	d1	d2	FLAG	d3	d4	ESC	ESC	ESC	d5	FLAG	d6

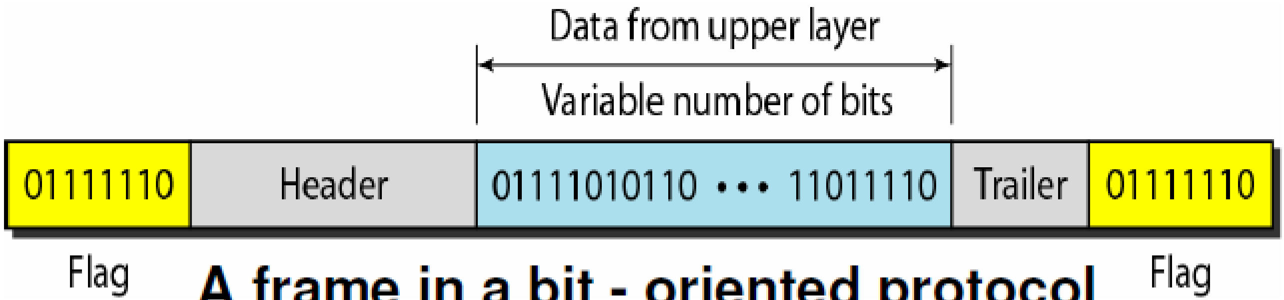
Data Link Control
Framing
Character - oriented Protocols
Byte stuffing : Example

BF4e11.11.13



Data Link Control
Framing
Bit - oriented Protocols
data section of a frame could be a sequence of bits to be interpreted as text, graphics, audio, video etc

most bit - oriented protocols use a special 8-bit pattern *01111110* (x7E) as the *flag*



A frame in a bit - oriented protocol

Data Link Control
Framing
Bit - oriented Protocols : bit stuffing

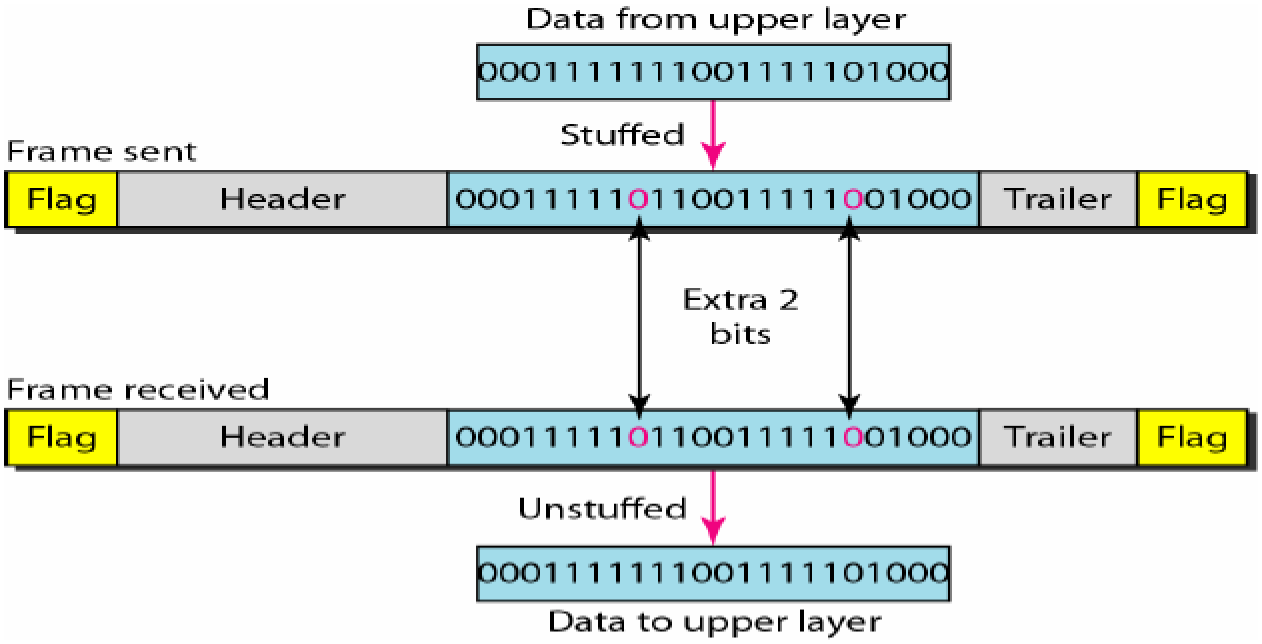
what happens if the pattern used for the flag also appears as part of data section ?

the receiver must be enabled to identify that this is not the end-of-frame

the problem is solved by ***bit stuffing*** where a single extra bit is introduced by the sender

if a 0 and ***five consecutive 1s*** are encountered, an ***extra 0*** is added by the sender
the extra 0 is eventually removed by the receiver

Data Link Control
Framing
Bit - oriented Protocols : bit stuffing



Data Link Control
Framing

Bit stuffing and destuffing : HDLC example

(a) Stream - 1

Data to be sent

011011111111111100

After stuffing and framing

*01111110*011011111011111000*01111110*

flag — bit stuff — bit stuff — flag

Bit-stuffing **avoids occurrence of the flag inside the frame**

stuff bit 0 after 11111s

(b) Stream - 2

Data received

0111111000011101111101111101100|01111110

After destuffing and deframing

00011101111-11111-110

111110…	**0 is SB**
1111110…	**flag**
1111111…	**error**

Data Link Control

Framing

Example : Bit-stuffing

Assuming a framing protocol that uses bit stuffing, show the bit sequence transmitted over the link when a frame contains the following bit sequence

01100111000111100000111101000001

Mark the stuffed bits

Data Link Control

Framing

Example : Bit-stuffing

PD 2.5

Assuming a framing protocol that uses bit stuffing, show the bit sequence transmitted over the link when a frame contains the following bit sequence

110101111101011111101011111110

Mark the stuffed bits

Data Link Control

Framing

Example : Bit-stuffing

PD 2.5

11010111110010111110101011111 0110

Data Link Control
Framing

Example : Bit-stuffing

PD 2.6

Suppose the following sequence of bits arrives at the receiver over a link :

11010111110101111110010111110110

Show the resulting frame after stuffed bits, if any, have been removed

Indicate any errors that might have been introduced into the frame. Defend your answer.

Data Link Control
Framing

Example : Bit-stuffing PD 2.6

1101011111*1011111*01011111*110

There was no error since 7 consecutive 1s were not received

Data Link Control

Framing

Example : Bit-stuffing

PD 2.6

1101011111*1011111*01011111*110

There was no error since 7 consecutive 1s were not received

Data Link Control
High-level Data Link Control (HDLC)

is a bit-oriented synchronous data link layer protocol

developed by the ISO

original ISO standards for HDLC are:

- ISO 3309 - Frame Structure
- ISO 4335 - Elements of Procedure
- ISO 6159 - Unbalanced Classes of Procedure
- ISO 6256 - Balanced Classes of Procedure

current standard : ISO 13239, replaces all the above standards

Data Link Control
High-level Data Link Control (HDLC)

is a bit - oriented protocol : for use over point-to-point and multipoint links
implements ARQ mechanisms

Configurations and Transfer modes

provides two common transfer modes that can be used in different configurations :

- normal response mode (NRM)
- asynchronous balanced mode (ABM)

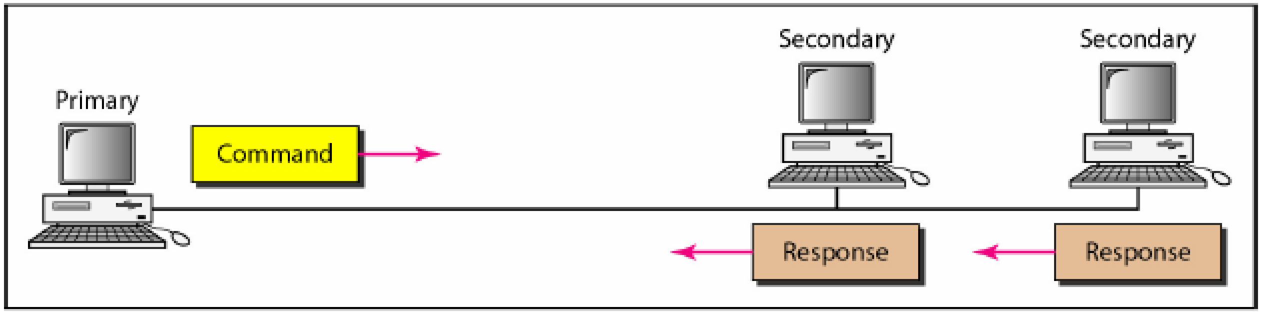
Data Link Control

High-level Data Link Control (HDLC)

Normal response mode

a. Point-to-point

un-balanced station configuration



b. Multipoint

Data Link Control

High-level Data Link Control (HDLC)

Normal response mode (NRM)

the station configuration is un-balanced

i.e. it comprises :

- one primary station that can send commands
- one or multiple secondary stations that can only respond

is used for both point-to-point and point-to-multipoint links

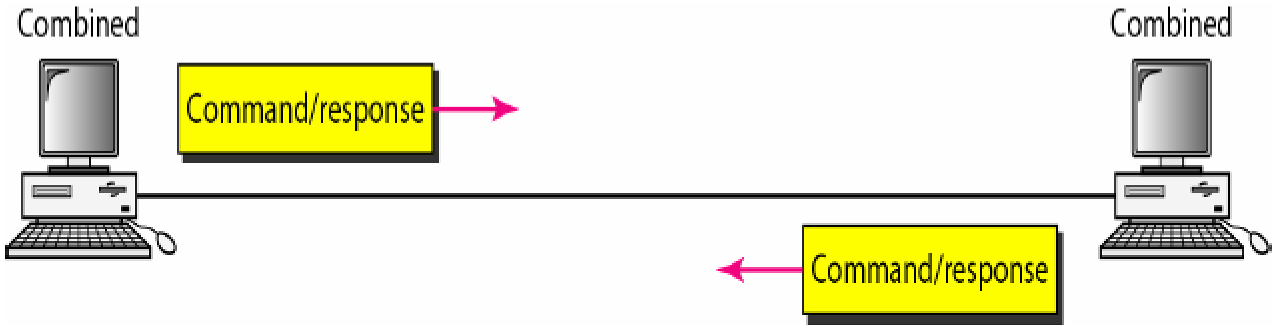
Data Link Control

High-level Data Link Control (HDLC)

Asynchronous balanced mode (ABM)

the configuration is balanced and point-to-point

each station can function as a primary or a secondary station (acting as peers)



balanced station configuration

Data Link Control

High-level Data Link Control (HDLC)

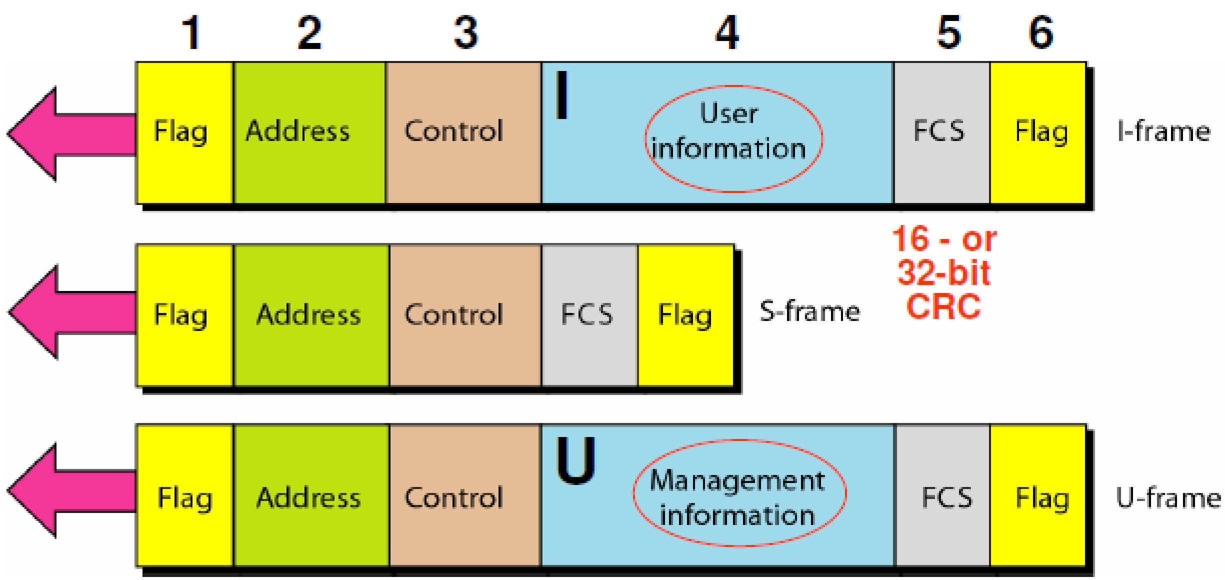
Frames

HDLC defines three types of frames :

- Information frames (I-frames) - used for transport of user data and related control information
- Supervisory frames (S-frames) - used for transporting only control information
- Unnumbered frames (U-frames) - used for carrying information intended for managing the link itself

Data Link Control
High-level Data Link Control (HDLC)
Frames : format

each frame may contain upto six fields



Data Link Control

High-level Data Link Control (HDLC)

Frames : format

Flag field

is an 8-bit sequence : 01111110

identifies both beginning and end of frame

serves as synchronization pattern for the receiver

in multiple-frame transmissions, ending flag of one frame can serve as the beginning flag of the next frame

Data Link Control

High-level Data Link Control (HDLC)

Frames : format

***Address* field**

contains the address of the *secondary* station

if primary station created the frame, it contains a *to* address

if secondary station created the frame, it contains a *from* address

length can be one byte (can identify upto 128 stations) or several bytes (for large networks)

Data Link Control

High-level Data Link Control (HDLC)

Frames : format

Address **field (contd.)**

if the address field is only one byte, the last bit is always 1

if the address field is more than one byte, all bytes except the last one will end with 0;

only the last one will end with 1

each intermediate byte with last bit = 0 indicates to the receiver that there are more address bytes to come

Data Link Control
High-level Data Link Control (HDLC)
Frames : format
Control field

is a 1- or 2- byte segment of the frame used for flow and error control

the interpretation of bits in this field depends on the frame type

more later

Data Link Control

High-level Data Link Control (HDLC)

Frames : format

***Information* field**

contains :

- **user data from network layer or**
- **management information**

length can vary from one network to another

***FCS* (frame check sequence) field**

is the HDLC error detection field

can contain 2- or 4-byte CRC $(x^{16} + x^{12} + x^{5} + 1)$

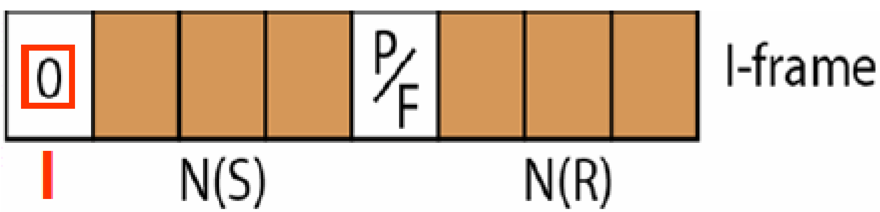
Data Link Control

High-level Data Link Control (HDLC)

Control field

determines the type of frame and its functionality

Control field for information or I-frames



for I frames, the first bit is 0

N(S) : 3 bits : define the sequence number of frame

Data Link Control

High-level Data Link Control (HDLC)

Control field for I-frames (contd.)

N(R) : 3 bits : correspond to the ack number when piggybacking is used

P/F : 1 bit : stands for poll / final

has meaning only when set to 1

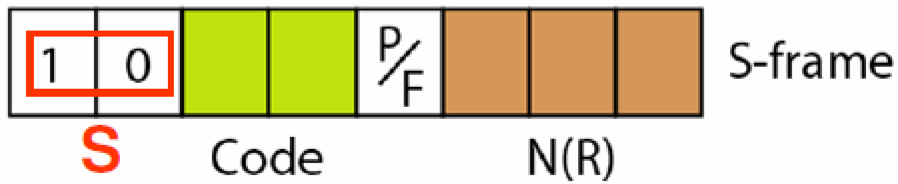
when frame, with the address field containing the address of the receiver, is sent by primary to secondary → *poll*

when frame, with the address field containing the address of the sender, is sent by secondary to primary → *final*

Data Link Control

High-level Data Link Control (HDLC)

Control field for supervisory or S-frames



for S frames, the first two bits are 10

are used for flow and error control

do not have information fields

N(R) : 3 bits : correspond to ACK or NAK number depending on the type of S-frame

Code : 2 bits : define the type of S-frame

Data Link Control

High-level Data Link Control (HDLC)

Control field for S-frames (contd.) : code

(a) Receive ready (RR) : code value = 00

used to acknowledge error-free receipt of the right frame or group of frames

N(R) defines ACK number

(b) Receive not ready (NRR) : code value = 10

acknowledges receipt of frame(s);

also announces that the receiver is busy and cannot receive any more frames

N(R) defines ACK number

Data Link Control

High-level Data Link Control (HDLC)

Control field for S-frames (contd.) : code

(c) Reject (REJ) : code value = 01

a NAK frame - used in Go-Back-ARQ to inform sender that last frame is lost or damaged

N(R) defines NAK number

(d) Selective reject (SREJ) : code value = 11

a NAK frame - used in Selective Repeat ARQ

N(R) defines NAK number

Data Link Control

High-level Data Link Control (HDLC)

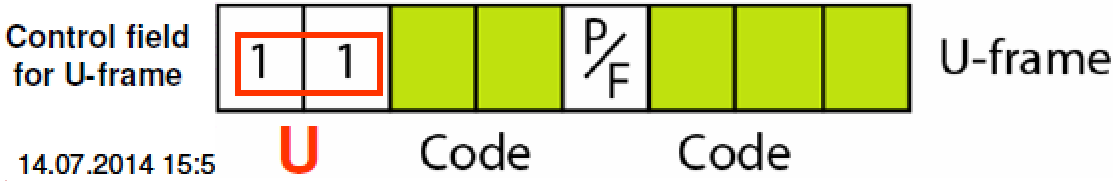
Control field for unnumbered or U-frames

used to exchange session management and control information between devices

U-frames contain information field, used for system management information

contains 2 + 3 bits of code field :

2-bit prefix before the P/F bit and 3-bit suffix after the P/F bit



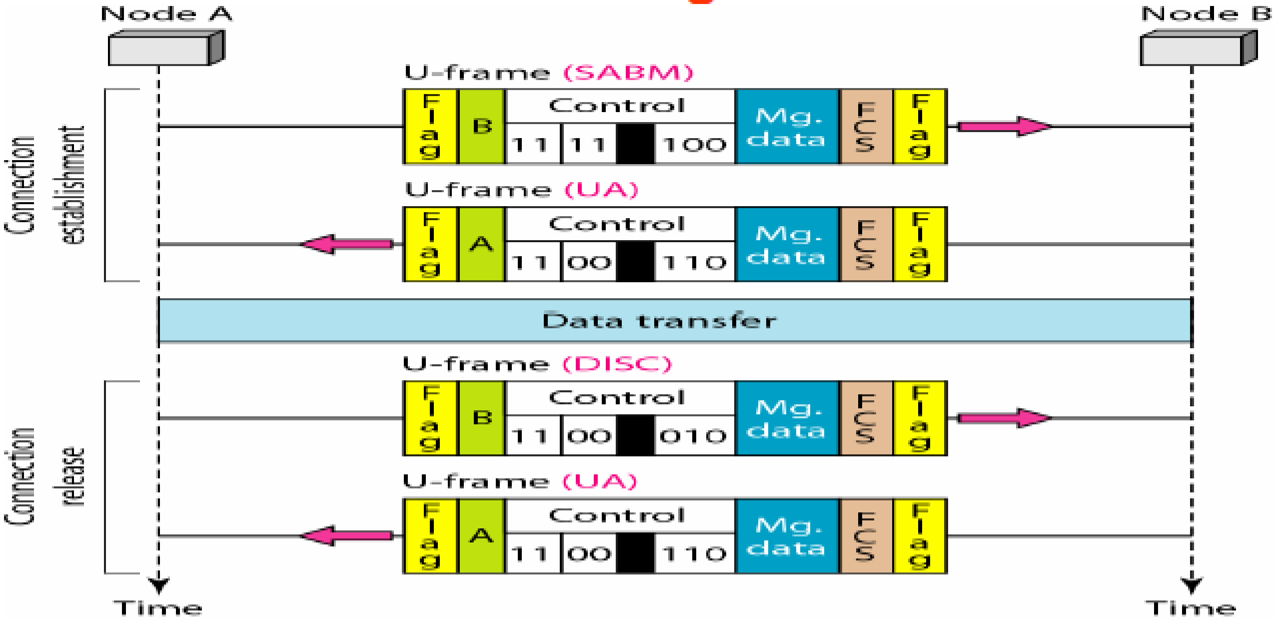
Data Link Control
High-level Data Link Control (HDLC)
U-frame control command and response

Code	*Command*	*Response*	*Meaning*
00 001	SNRM		Set normal response mode
11 011	SNRME		Set normal response mode, extended
11 100	SABM	**DM**	Set asynchronous balanced mode or **disconnect mode**
11 110	SABME		Set asynchronous balanced mode, extended
00 000	UI	**UI**	Unnumbered information
00 110		**UA**	**Unnumbered acknowledgment**
00 010	DISC	**RD**	Disconnect or **request disconnect**
10 000	SIM	**RIM**	Set initialization mode or **request information mode**
00 100	UP		Unnumbered poll
11 001	RSET		Reset
11 101	XID	**XID**	Exchange ID
10 001	FRMR	**FRMR**	Frame reject

Data Link Control

High-level Data Link Control (HDLC)

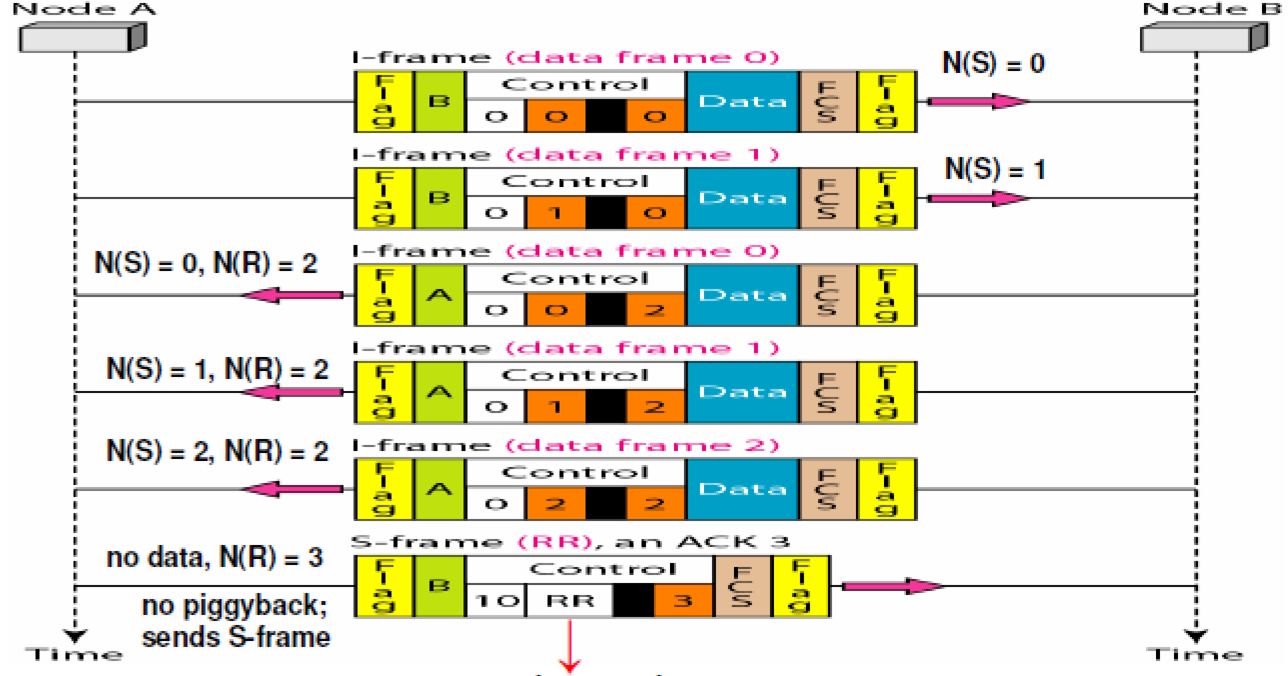
Example of connection establishment and connection release using U-frames



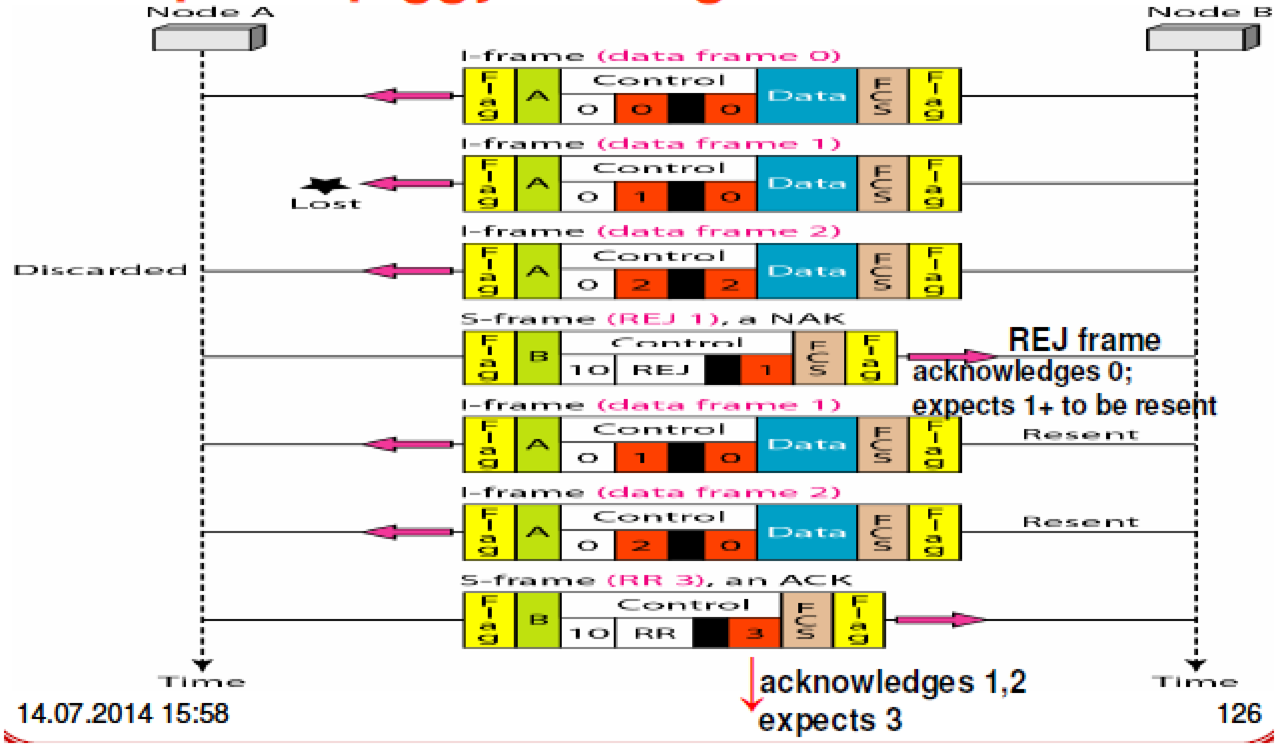
Data Link Control

High-level Data Link Control (HDLC)

Example of piggybacking without error



Data Link Control
High-level Data Link Control (HDLC)
Example of piggybacking with error



Data Link Control

Point - to - Point Protocol

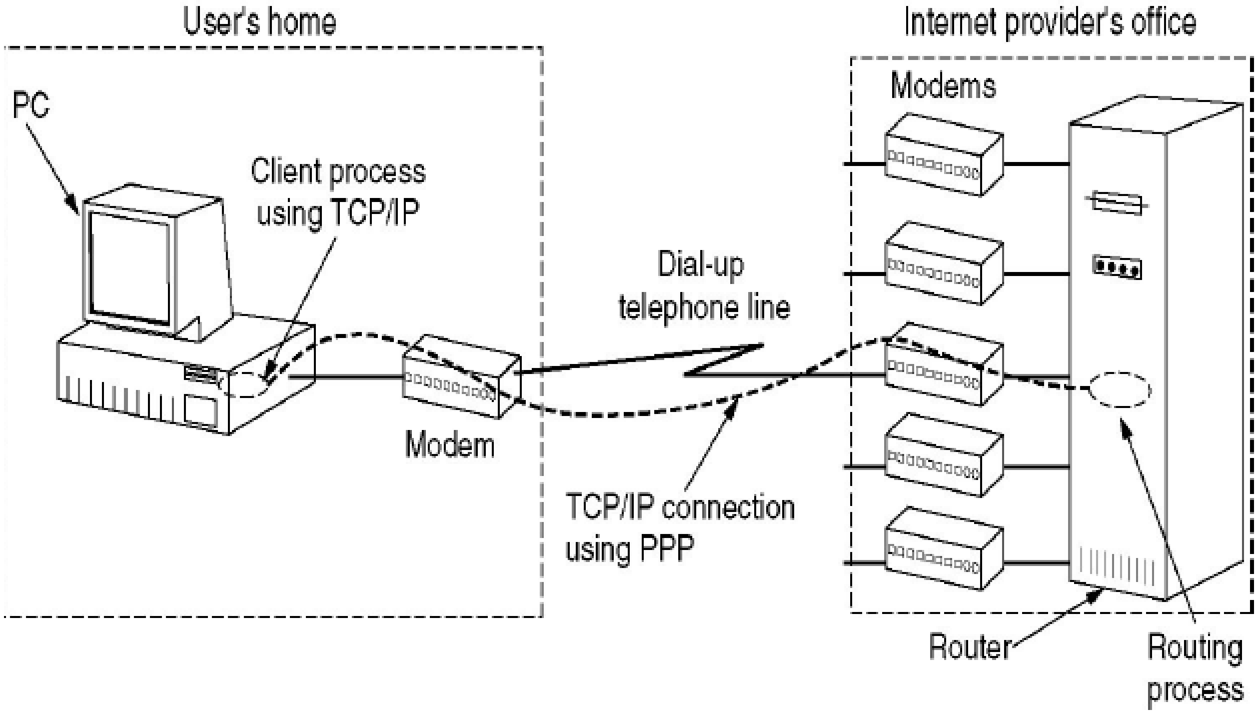
one of the most common protocols used for point-to-point access

used to connect home computers to the server of an ISP

physical layer : modem connected to the Internet through a telephone line

data link layer : protocol is required to control and manage transfer of data

Data Link Control
Point - to - Point Protocol



Data Link Control

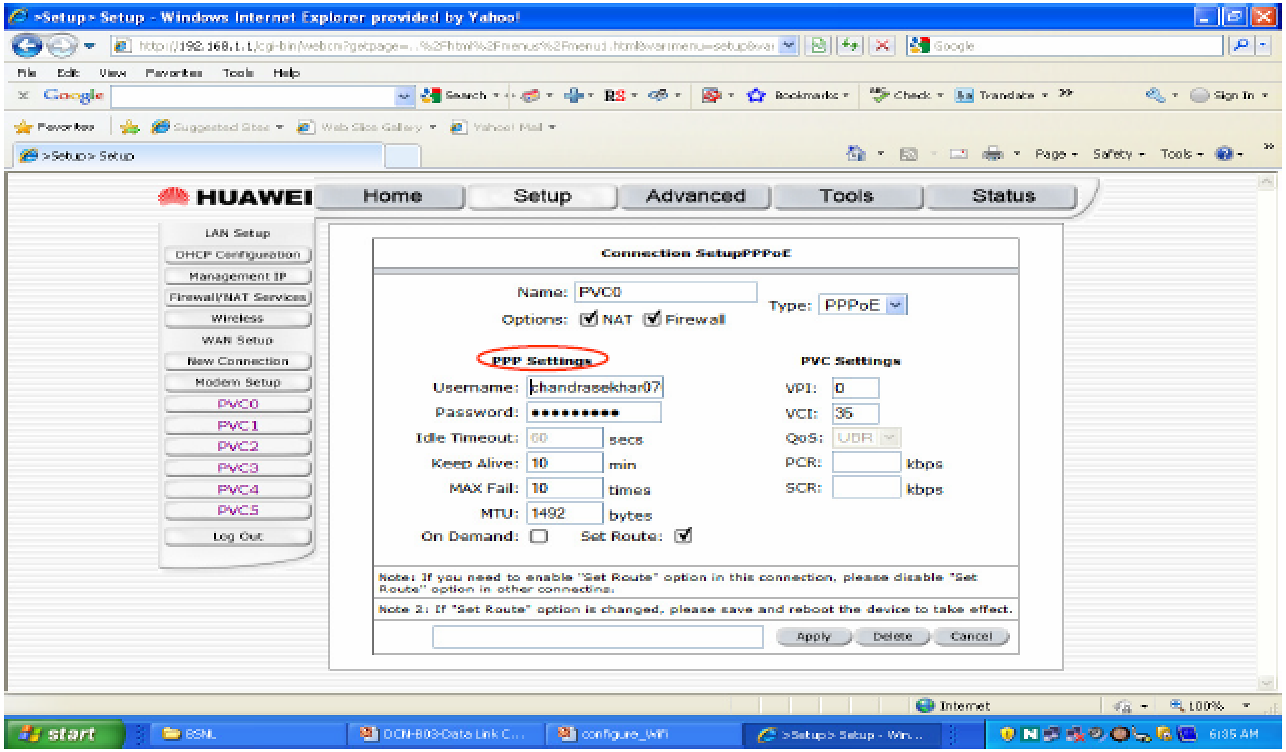
Point - to - Point Protocol

PPP provides several services :

- defines format of the frame
- defines how two devices can negotiate establishment of link and exchange data
- defines how network layer data are encapsulated in the datalink frame
- defines how two devices can authenticate each other

Data Link Control

Point - to - Point Protocol



Data Link Control

Point - to - Point Protocol

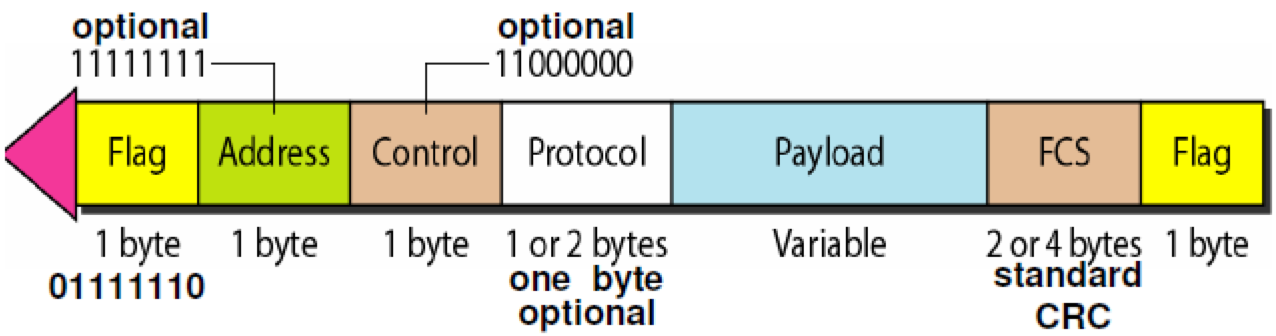
other issues :

- does not provide flow control
- error control limited to detection; uses CRC
- if frame is corrupted, it is discarded
- lack of error control and sequence numbering may cause out-of-order receipt of frames
- does not provide sophisticated addressing mechanism to handle frames in multipoint configurations

Data Link Control

Point - to - Point Protocol

Framing : PPP frame format



PPP is byte - oriented

uses 01111101 as the ESC byte for stuffing

protocol field : defines type of data being carried viz. user data or other information

Data Link Control

Point - to - Point Protocol

Framing : PPP frame format

Payload field :

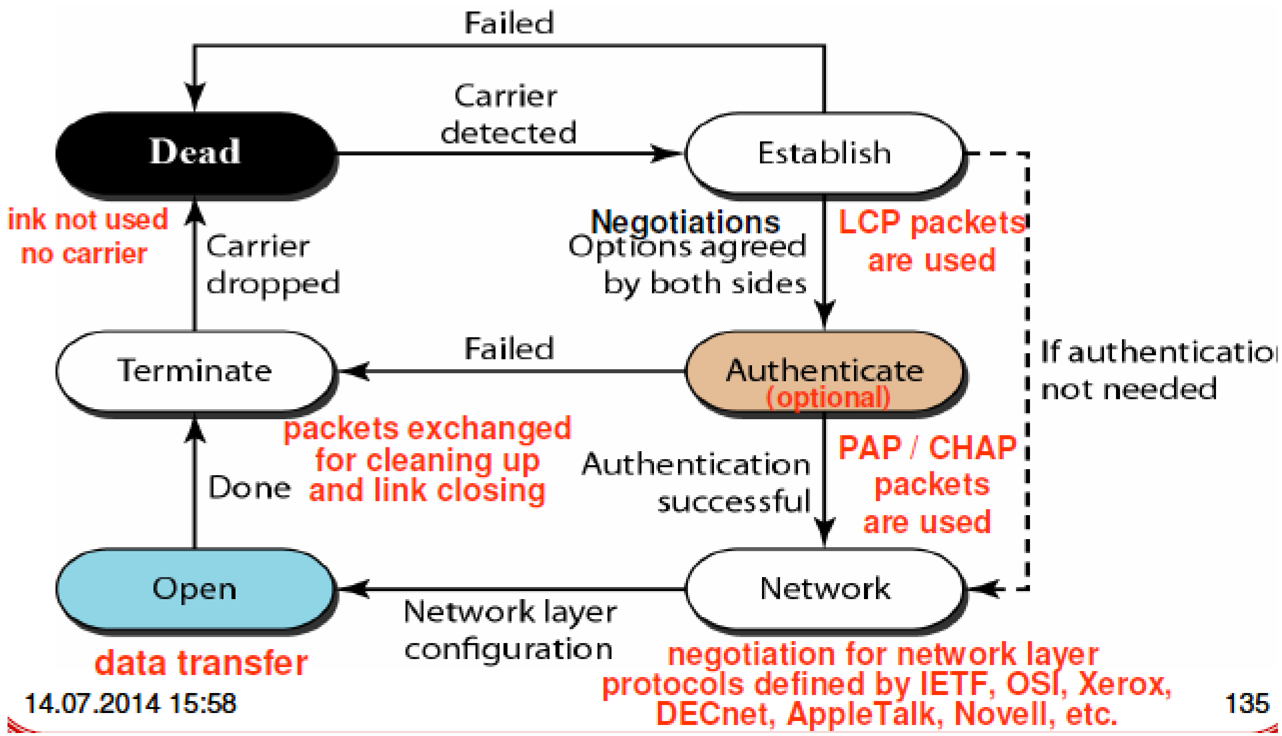
carries user data or other information

data field is a sequence of bytes .. default maximum of 1500 bytes .. can be changed during negotiation

byte stuffing is used

data padding is used if the size is less than the maximum default value or the maximum negotiated value

Data Link Control
Point - to - Point Protocol
Transition phases

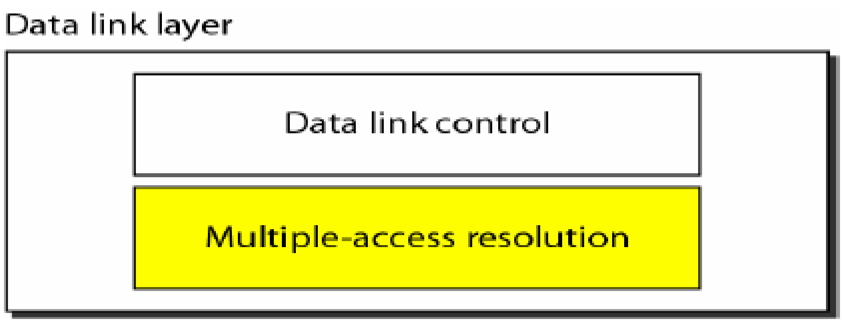


Media Access Control

provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multipoint network

Ex. : LAN

data link layer can be considered as two sublayers :



Media Access Control

when nodes or stations are connected and use a common link,…..

i.e. multipoint or broadcast link, …..

multi-access protocol to coordinate access to the link is required

the procedures must ensure the following :

- right to access the link
- no two nodes access the link at the same time
- nodes do not interrupt each other
- node does not monopolize the use of link

Media Access Control

Random Access

also called contention methods
no station is superior to another station
no station permits or denies permission to another station to send
at each instance, a station that has data to send, uses a procedure defined by a protocol to decide whether or not to send
the decision to send is based on the state of the medium, i.e. idle or busy, and the station has to ascertain this state

Media Access Control

Random Access

also called contention methods
no station is superior to another station
no station permits or denies permission to another station to send
at each instance, a station that has data to send, uses a procedure defined by a protocol to decide whether or not to send
the decision to send is based on the state of the medium, i.e. idle or busy, and the station has to ascertain this state

Media Access Control

Random Access

each station can transmit when it desires….. on the condition that it follows the predefined procedure,

including the testing of the state of the medium

there is no scheduled time for a station to transmit

transmission is *random* amongst stations

no rules specify which station should send next

stations *compete* with one another to access the medium

Media Access Control
Random Access

if more than one station tries to send, access conflict or *collision* will result → frames will be destroyed / modified

issues to be considered to handle collision :

- when can the station access the medium ?
- what can the station do if the medium is busy ?
- how can the station determine the success or failure of transmission ?
- what can the station do if there is an access conflict ?

Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)

objective :

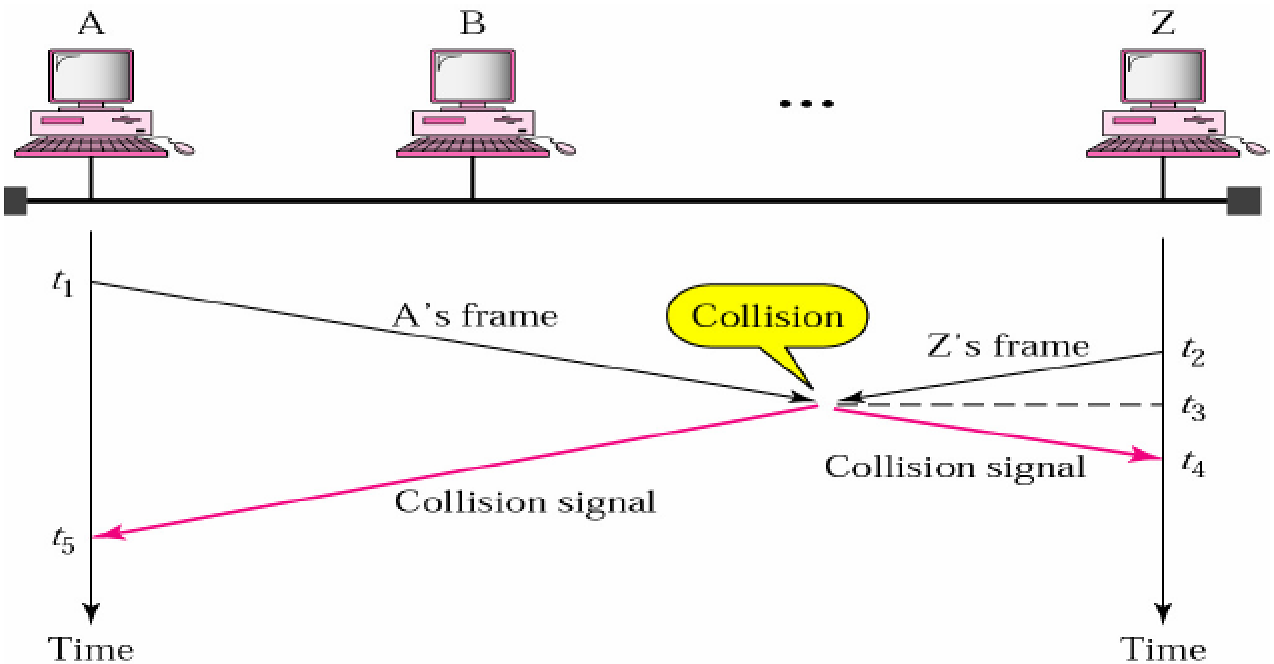
to minimize the chance of collision and therefore, increase performance …..

station senses the state of the medium before sending

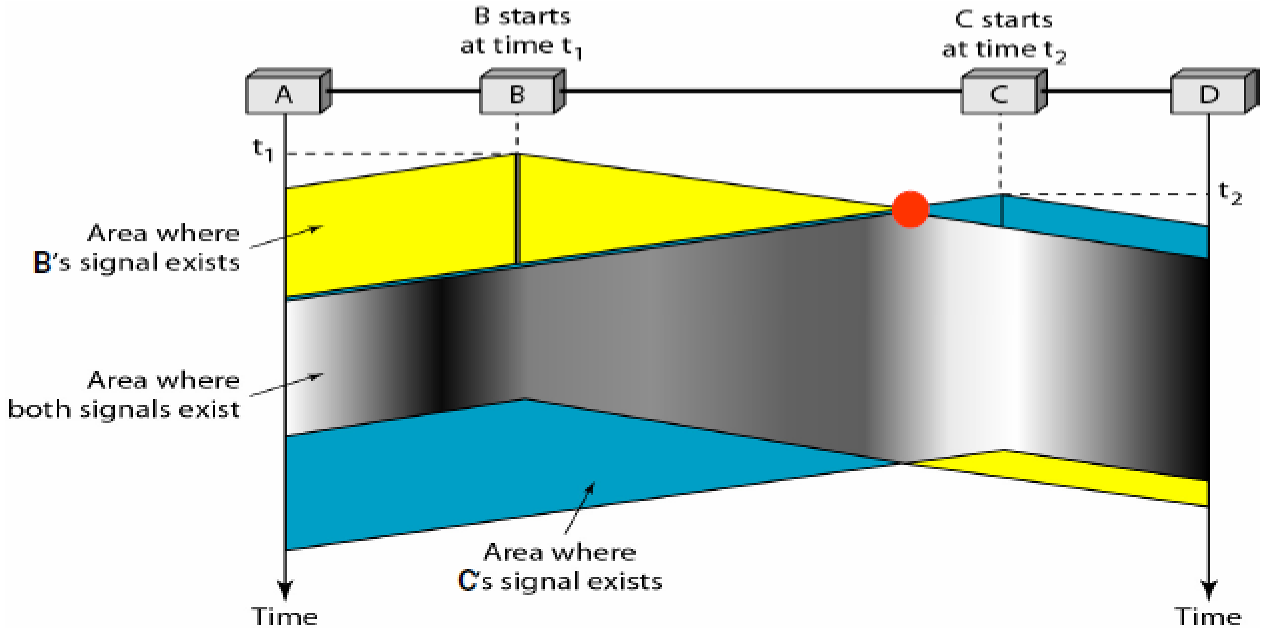
(sense before transmit or listen before talk)

CSMA can reduce the possibility of collision, but not eliminate it

Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)

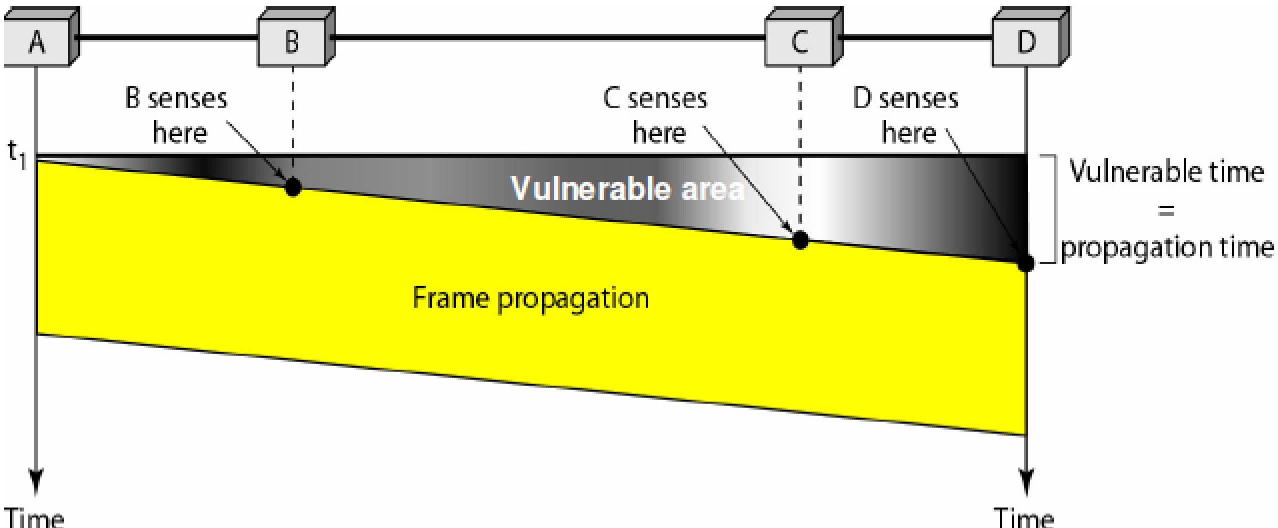


Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)



Space and Time model of collision in CSMA

Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)
Vulnerable time : the length of time during which there is a possibility of collision



Vulnerable Time in CSMA

Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)
Persistence methods

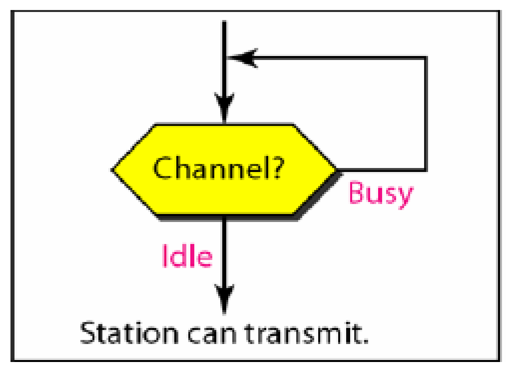
to deal with the *action a station needs to take* when a channel is busy or idle

three methods have been devised :

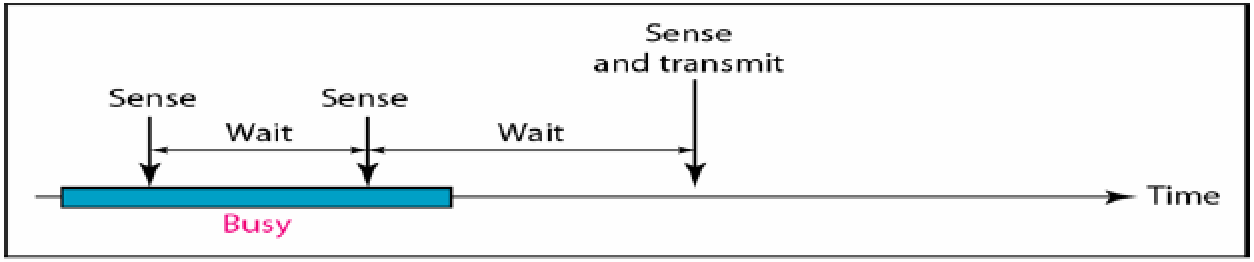
- the 1 - persistent method
- the non - persistent method
- the p - persistent method

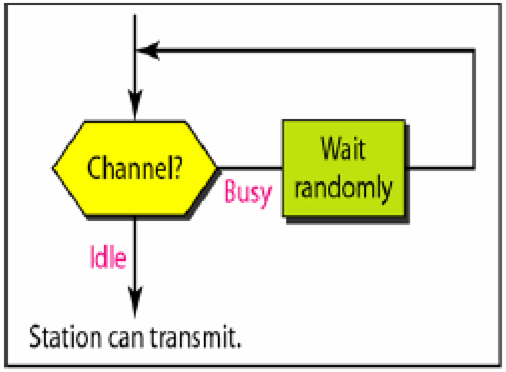
Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)
Persistence methods : 1 - persistent method

after the station finds the line idle, it transmits immediately,
with probability = 1
has the highest chance of collision



Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)
Persistence methods : non - persistent method





Media Access Control

Random Access

Carrier Sense Multiple Access (CSMA)

Persistence methods : non - persistent method

a station that has a frame to send senses the line

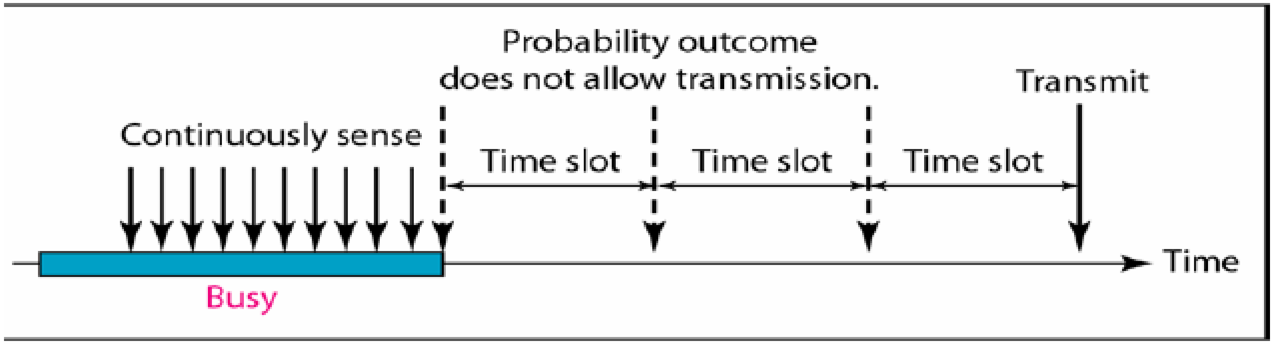
if the line is idle, it transmits immediately

if the line is not idle, it waits for a random amount of time and then senses the line again

reduces chance of collision, since waiting period is random for different stations

reduced efficiency, since medium may remain idle even when stations have frames to be sent

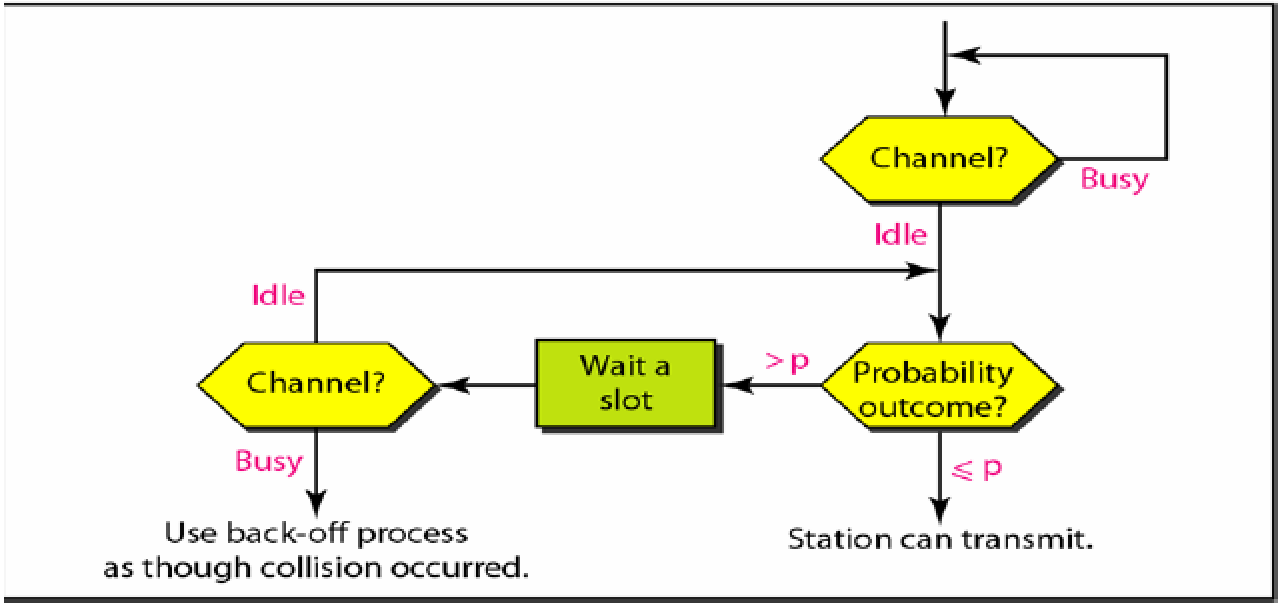
Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)
Persistence methods : p - persistent method



combines the advantages of the other two strategies

reduces chance of collision and improves efficiency

Media Access Control
Random Access
Carrier Sense Multiple Access (CSMA)
Persistence methods : p - persistent method



Media Access Control

Random Access

Carrier Sense Multiple Access (CSMA)

Persistence methods : p - persistent method

1. station senses the channel
2. if idle :

(a) sends frame with probability p or

(b) waits for the beginning of the next time slot and senses channel again

3. if idle, goes to step 2
4. if busy, station acts as though collision has occurred and uses the back-off procedure

Media Access Control

Random Access

CSMA with Collision Detection (CSMA / CD)

CSMA does not specify procedure to handle collision

CSMA / CD provides for handling collision
a station monitors the medium after it sends a frame to see if the transmission was successful

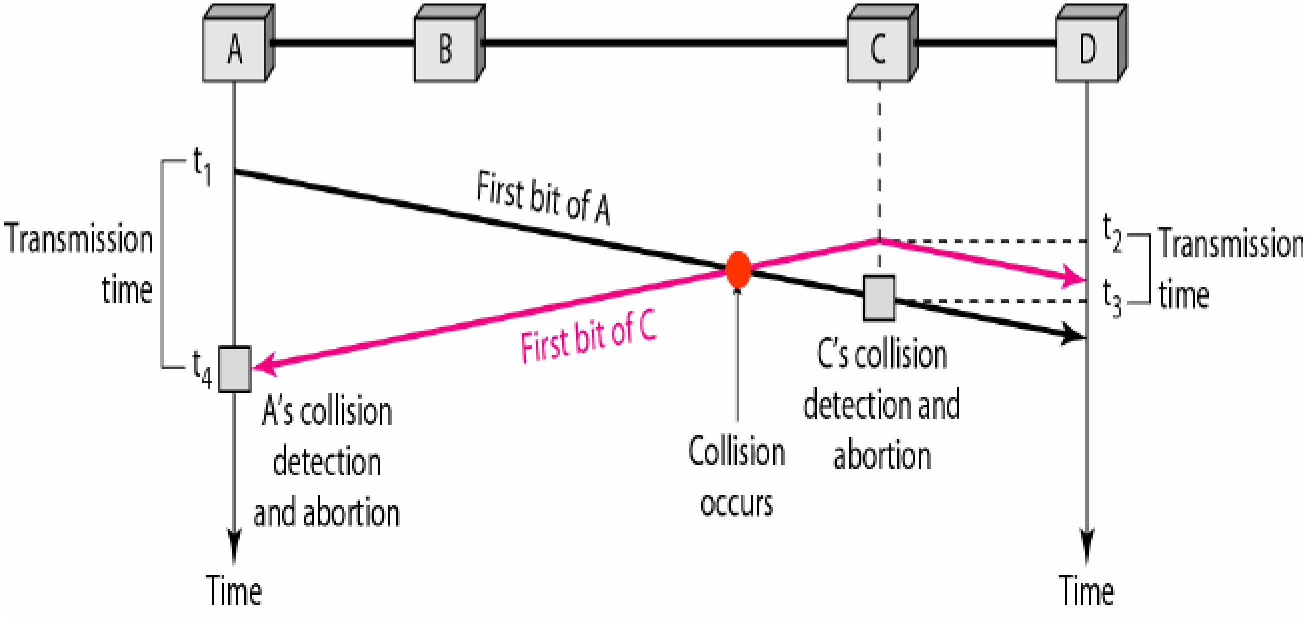
if there is collision, the frame is resent

Media Access Control

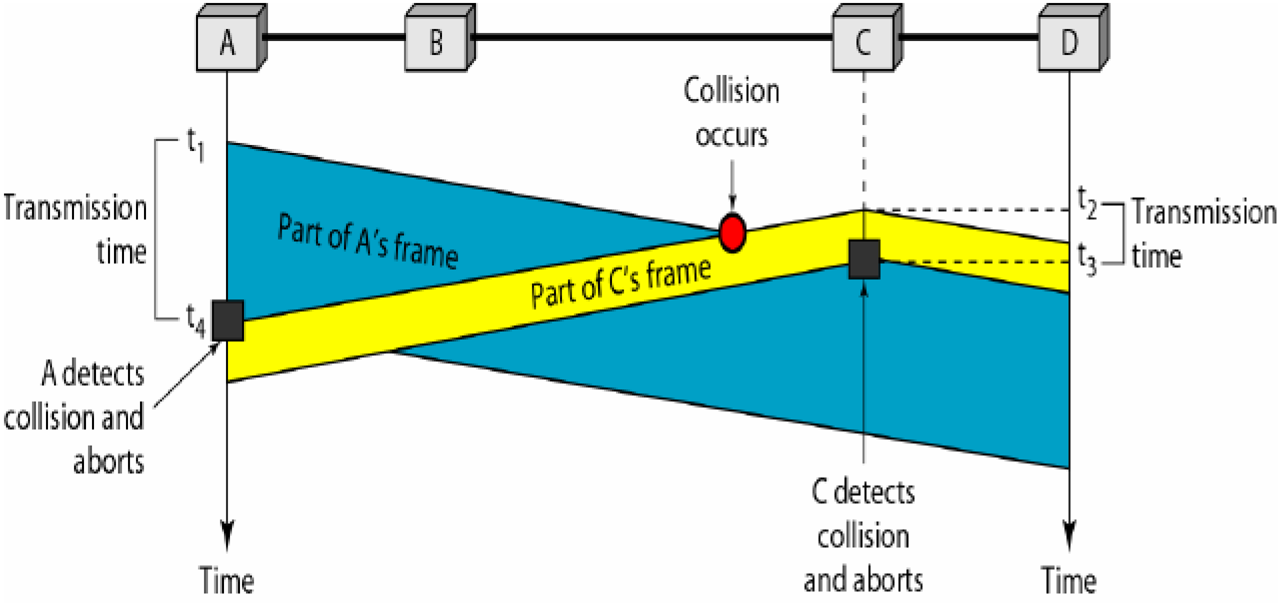
Random Access

CSMA with Collision Detection (CSMA / CD)

Collision of the first bit in CSMA / CD



Media Access Control
Random Access
CSMA with Collision Detection (CSMA / CD)
Collision and abortion in CSMA / CD



Media Access Control

Random Access

CSMA with Collision Detection (CSMA / CD)

Minimum frame size

in CSMA / CD, once an entire frame is sent, the sending station :

- does not keep a copy of the frame
- does not monitor the line for detecting collision

before sending the last bit of the frame, the sending station must detect collision

if there is collision, transmission must be aborted

Media Access Control
Random Access
CSMA with Collision Detection (CSMA / CD)
Minimum frame size (contd.)

if two stations, involved in a collision ….
are separated by the farthest distance
such that the propagation time (one-way)
between them is T_p ….
in the worst case scenario, the signal
from the first station takes T_p to reach the
second station and ….
the effect of collision takes another T_p to
reach the first station

Media Access Control

Random Access

CSMA with Collision Detection (CSMA / CD)

Minimum frame size (contd.)

to detect collision before the last bit is sent, the sending station must still be transmitting after $T_{fr} = 2 \times T_p$

the (minimum) frame size must be big enough to facilitate the above

Media Access Control

Random Access

CSMA with Collision Detection (CSMA / CD)

Minimum frame size (contd.)

Example BF4e12.5

Given bandwidth = 10 Mbps

Maximum T_p = 25.6 microseconds

Minimum size of frame

= 10 Mbps x 2 x 25.6 microseconds

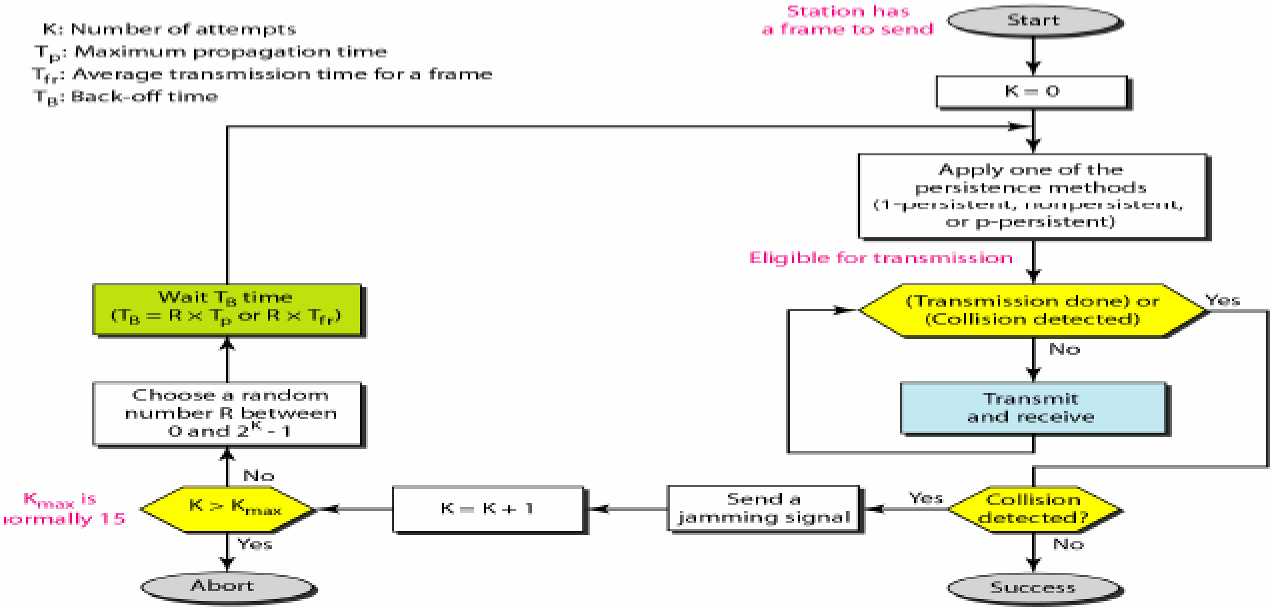
= 512 bits = 64 bytes

Media Access Control

Random Access

CSMA with Collision Detection (CSMA / CD)

Procedure

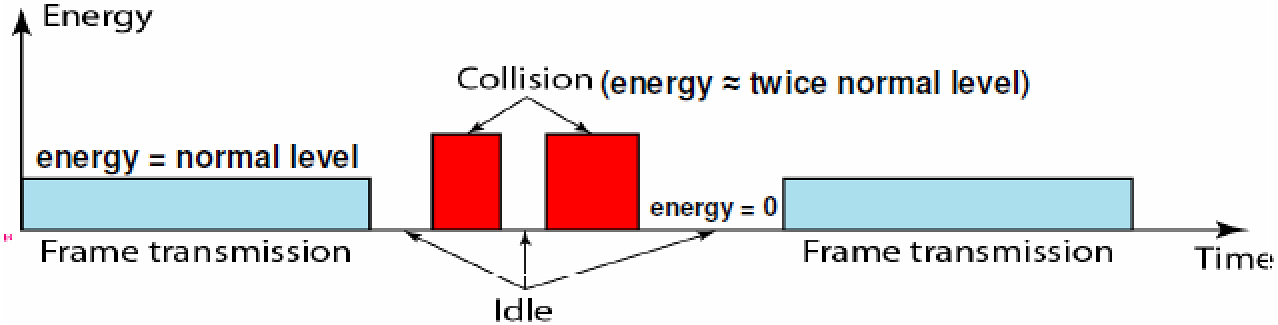


Media Access Control
Random Access

CSMA with Collision Detection (CSMA / CD)

Energy levels

a station that has a frame to send or is sending a frame …. needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode



Media Access Control

Random Access

CSMA with Collision Avoidance (CSMA / CA)

in CSMA / CD, when there is no collision, the sender receives one (*its own*) signal
when there is collision, two signals are received : its own signal + signal of a second station
in a wired network, the second signal has almost the same energy as the original (either cable is short or repeater is used)
and hence the sending station can easily distinguish between the two

Media Access Control
Random Access
CSMA with Collision Avoidance (CSMA / CA)

in case of a ***wireless network***, much of the sent energy is lost in transit →
the received signal has very low energy
→ not adequate for effective collision detection
collisions need to be ***avoided*** because they cannot be easily detected
collisions are avoided through the use of three strategies : → →

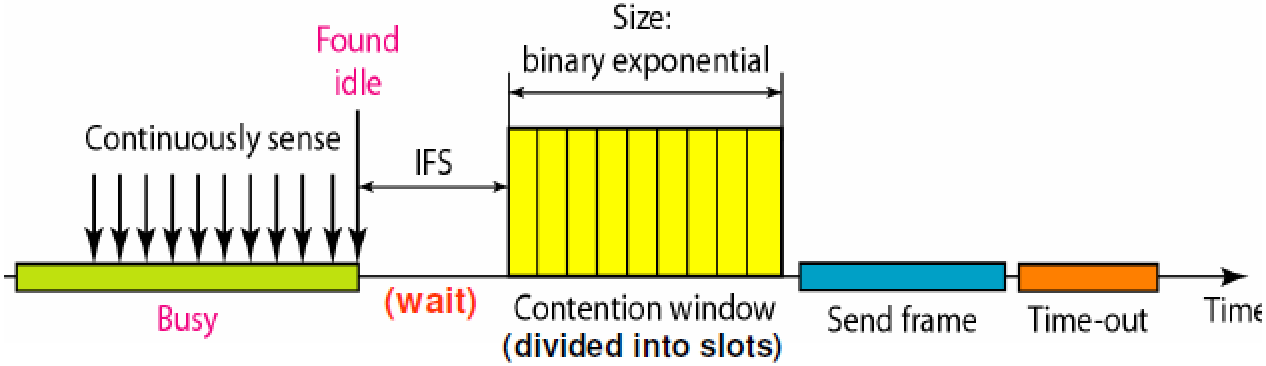
Media Access Control

Random Access

CSMA with Collision Avoidance (CSMA / CA)

three strategies :

- **inter frame space (IFS)**
- **contention window**
- **acknowledgements**



Media Access Control

Random Access

CSMA with Collision Avoidance (CSMA / CA)

Inter frame space (IFS)

even if the channel is found idle, collisions are avoided by *waiting* for a period of time called the IFS

the IFS time allows the front of the signal transmitted by the distant station to reach the station waiting on its IFS time

IFS variable can also be used to prioritize stations or frame types by allocating a shorter IFS for higher priority

Media Access Control

Random Access

CSMA with Collision Avoidance (CSMA / CA)

Contention window

is an amount of time divided into slots

a station, that is ready to send, waits for a random number of slots *after the IFS*

the number of slots in the window changes according to the binary exponential back - off strategy →

set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS frame

Media Access Control

Random Access

CSMA with Collision Avoidance (CSMA / CA)

Acknowledgement

positive acknowledgement and a time-out timer are used to ensure that the receiver has received the frame

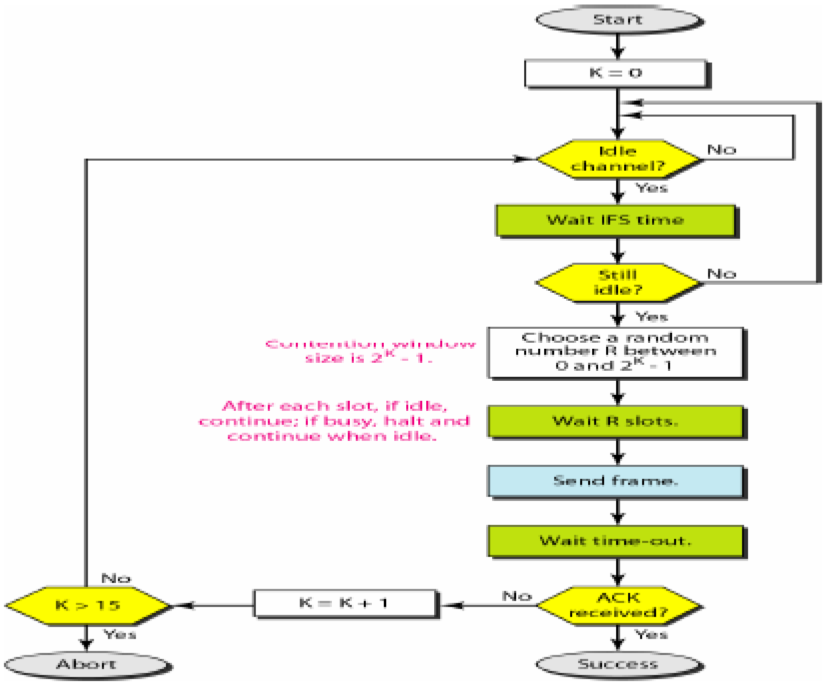
Procedure used by CSMA / CA:

flow diagram → →

Media Access Control

Random Access

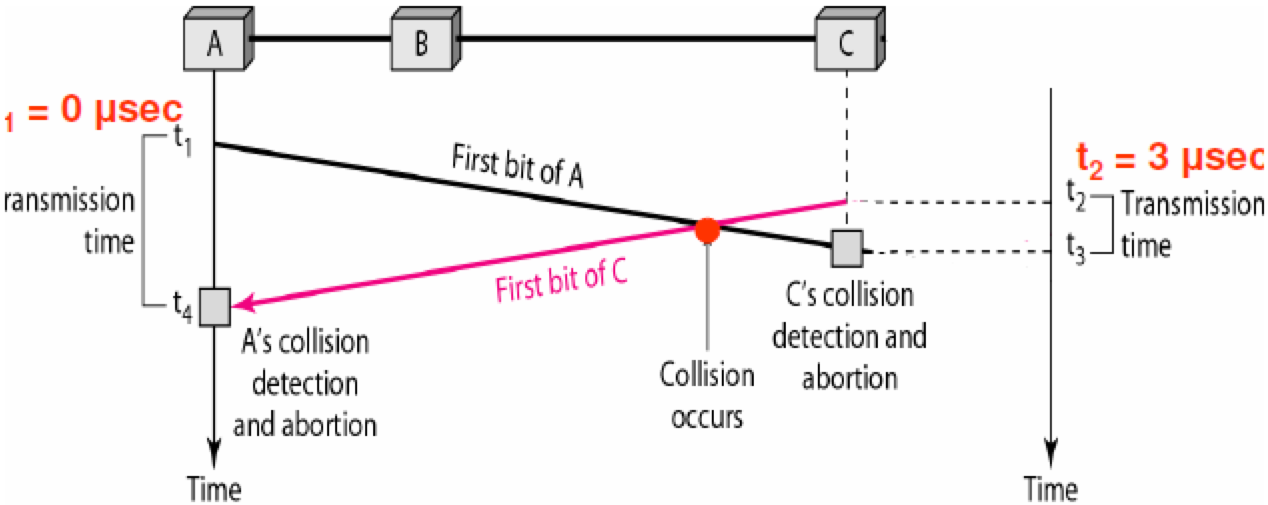
CSMA / CA flow diagram



Media Access Control
Random Access

CSMA / CD Example

BF4e12.7.17



Distance A to C = 2 Km

Data rate A to C = 10 Mbps

Media Access Control
Random Access

CSMA / CD Example BF4e12.7.17

Given :

data rate = 10 Mbps;

A to C distance = 2 Km @ 2 x 10^5 Km / sec;

t_1 = 0 µsec and t_2 = 3 µsec;

size of the frame is long enough to guarantee the detect of collision by both stations A and C.

Find : → →

Media Access Control
Random Access

CSMA / CD Example BF4e12.7.17

(a) $(t_3 - t_1) = (2 \text{ Km} \div 2 \times 10^5 \text{ Km / sec})$

$= 10\ \mu\text{sec} \rightarrow t_3 = t_1 + 10\ \mu\text{sec}$

$\rightarrow t_3 = 10\ \mu\text{sec}$

(b) $(t_4 - t_2) = 10\ \mu\text{sec} \rightarrow t_4 = t_2 + 10\ \mu\text{sec}$

$\rightarrow t_4 = 13\ \mu\text{sec}$

(c) A transmits for 13 μsec @ 10 Mbps →

A transmits 13 μsec x 10 Mbps = 130 bits

(d) C transmits for 7 μsec @ 10 Mbps →

A transmits 7 μsec x 10 Mbps = 70 bits